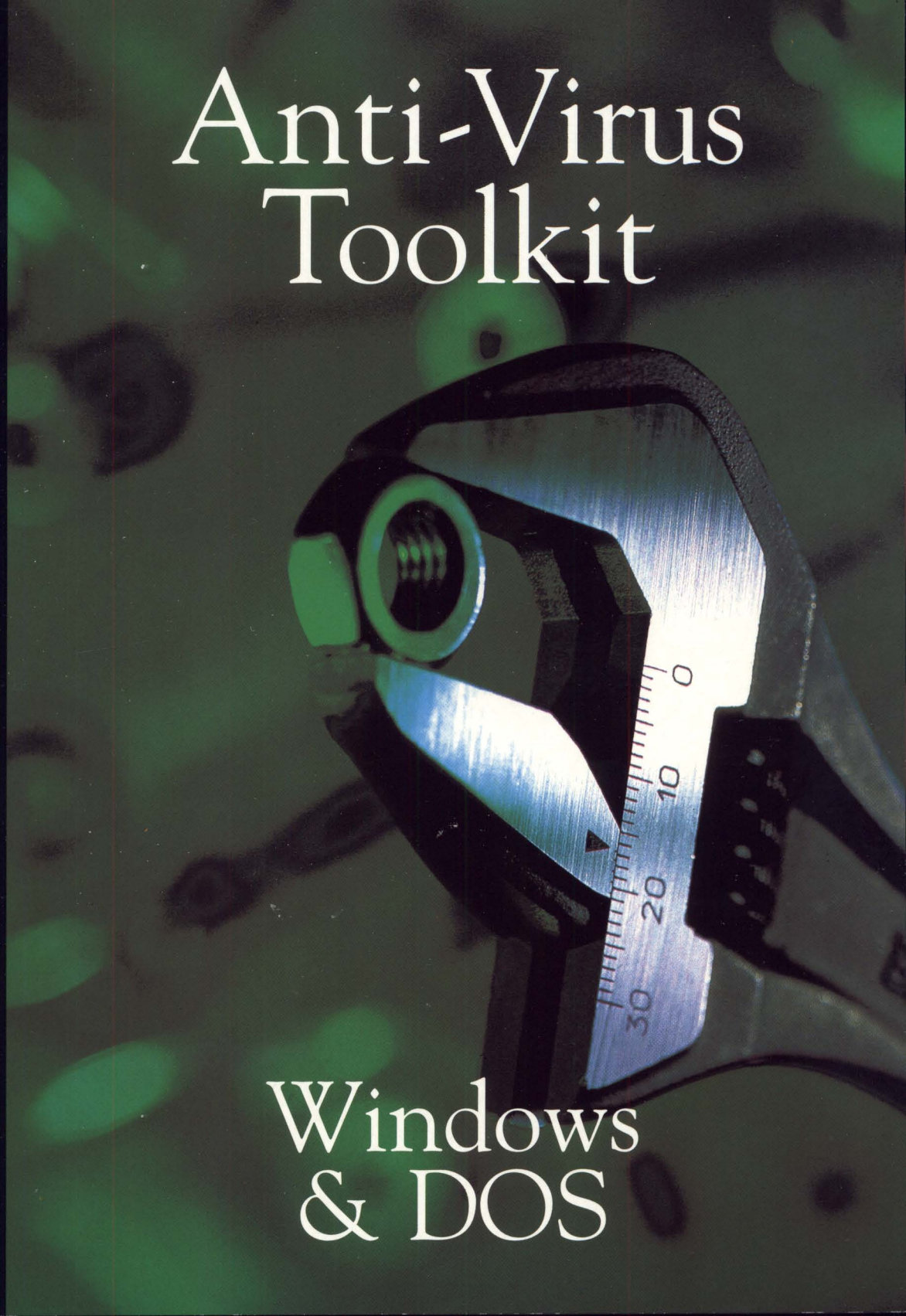
DR SOLOMON'S

# Anti-Virus Toolkit



# Windows & DOS

# Dr Solomon's
# Anti-Virus Toolkit
## for Windows and DOS

**S&S International PLC**
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK
Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777
E-mail: support@drsolomon.com

**S&S Software International, Inc.**
17 New England Executive Park, Burlington, MA 01803, USA
Tel: +1 617 273 7400 Fax: +1 617 273 7474
E-mail: support@us.drsolomon.com

**S&S International (Deutschland) GmbH**
Luisenweg 40, 20537 Hamburg, Deutschland
Telefon: +49 (0)40 2519 54-0 Fax: +49 (0)40 2519 54-50
E-mail: support@de.drsolomon.com

**CompuServe:** GO DRSOLOMON
**World Wide Web:** http://www.drsolomon.com/

SS1110A-20-05-7.0

## Copyright

**Dr Solomon's Anti-Virus Toolkit for Windows and DOS** is copyright © 1993,1994, 1995 S&S International PLC. All rights reserved. Dr Solomon's Anti-Virus Toolkit for Windows and DOS is not copy-protected. This does not mean that you can make unlimited copies of it. Dr Solomon's Anti-Virus Toolkit for Windows and DOS is protected by the copyright laws which pertain to computer software. It is illegal to make copies of the program other than as may be licensed or for purposes of backup without written permission from S&S International PLC. No part of the manual or other documentation accompanying Dr Solomon's Anti-Virus Toolkit for Windows and DOS may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form or by any means, without the prior written permission of S&S International PLC.

## Disclaimer

Neither S&S International PLC nor anyone else who has been involved in the creation, production or delivery of Dr Solomon's Anti-Virus Toolkit for Windows and DOS or this manual makes any warranties with respect to the contents of the software or this manual and each specifically disclaims any implied warranties to the extent allowed by legislation. S&S International PLC reserves the right to revise the software and the manual and to make changes from time to time in the contents without obligation to notify any person.

## Trademarks

Dr Solomon's is a registered trademark of S&S International PLC. All other product names mentioned are acknowledged to be the marks of their producing companies.


## Software release

This manual describes Version 7.5 of Dr Solomon's Anti-Virus Toolkit for Windows and Dr Solomon's Anti-Virus Toolkit for DOS.


## Manual edition

Edition 3.0
November 1995

# Quickstart

**If you need to act quickly, read these pages, especially if you think you may have a virus.**

## Quick Virus Check

If you have bought the Toolkit because you suspect you might have a virus, the most important things to remember are:

- Don't panic.
- Don't rush into anything.

You could end up causing more damage than the virus.

If you want to check for viruses straight away, run FindVirus. You do not have to install the Toolkit on your PC to do this. Follow the procedure below.

1. Switch off the PC.
2. Insert a virus-free, write-protected, DOS system diskette in the A drive and switch on the PC.

   Ideally, you should use the system disk that was supplied with your PC or your latest operating system upgrade.
3. When the system prompt appears, insert the Toolkit diskette containing FINDVIRU.EXE into the drive. This is usually, but not always, the diskette labelled Installation Disk 1 for the DOS Anti-Virus Toolkit. You can use the DIR command to check.
4. Change to that drive by typing `A:` or `B:` as appropriate. Press ↵.
5. Now type `FINDVIRU /LOCAL.` Press ↵.

   FindVirus will scan your local drives for viruses. If it finds a virus, it displays the virus name on the screen.

## Quick Repair

If you do have a virus, the simplest way to remove it is as follows:

1. Boot from a clean, write-protected, DOS system diskette.
2. At the system prompt, insert the disk containing FINDVIRU.EXE into the appropriate drive and change to it by typing `A:` or `B:`. Press ↵.
3. Type `FINDVIRU /REPAIR /LOCAL`. Press ↵.
4. The screen displays a list of the files infected. Where possible, files are repaired, otherwise they are renamed.
5. Type `FINDVIRU /LOCAL /ANALYZE`. Press ↵.

## Quick Installation

To install the Toolkit on your hard disk, follow these steps:

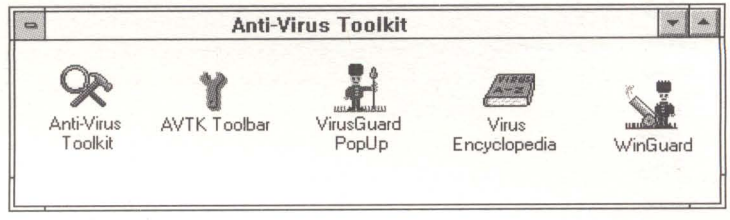
1. Boot the PC from a clean, write-protected, DOS system diskette.
2. To install the DOS Toolkit, insert Installation Disk 1 for the DOS Anti-Virus Toolkit in the A: drive. Type `INSTALL` and press ↵.
3. The Windows Toolkit must be installed from DOS as it cannot be installed from within Windows.

   Insert the Installation Disk 1 for the Windows Anti-Virus Toolkit in the A: drive. Type `SETUP` and press ↵. If you install the Windows version, the DOS version is also installed, since some programs must be run from DOS.

4. Follow the on-screen instructions carefully. You will be prompted to install VirusGuard and WinGuard, the Toolkit's primary memory-resident programs.
   VirusGuard provides memory-resident protection under DOS. WinGuard provides memory-resident protection under Windows. Installation is strongly recommended.

To run the DOS Toolkit, change to the Toolkit directory and type `TOOLKIT`. Press ↵.

For the Windows Toolkit, the Anti-Virus program group will be created automatically the next time you run Windows:




To run the Toolkit, double-click on the Anti-Virus Toolkit icon.

For extra security, you can run the Toolkit from diskette. Insert the diskette containing TOOLKIT.EXE, change to the drive and type `TOOLKIT`.

# Contents

**Contents** ..... vii

**Preface** ..... xv
How to use this manual ..... xv
Conventions ..... xvii
What you need ..... xviii
The Windows and DOS versions ..... xix
Using a mouse ..... xix
Using the keyboard ..... xx
Dialog boxes ..... xxi
File selection ..... xxii
Windows icons ..... xxiii
Windows Toolbar ..... xxiv
On-line help ..... xxvi
Related documentation ..... xxvii
The Virus Encyclopedia ..... xxvii
Other versions of the Toolkit ..... xxvii
Registration and upgrades ..... xxix
If you need help ..... xxx

**1. Introduction** ..... 1
1.1 What is a virus? ..... 1
1.2 Types of virus ..... 2
File viruses ..... 2
Macro viruses ..... 3
Boot and partition sector viruses ..... 3
Companion viruses ..... 4
Overwriting viruses ..... 5
Multipartite viruses ..... 5
Droppers ..... 5
1.3 Characteristics of viruses ..... 5
Stealth ..... 5
Polymorphism ..... 5
Virus names ..... 6
Variants ..... 6
How viruses spread ..... 6
1.4 Other potential problems ..... 7
Bugs ..... 7
Low-level software clashes ..... 8
Trojans ..... 8
Time bombs and logic bombs ..... 9

Jokes ..... 9
Human Error ..... 9
1.5 What you can do ..... 10
Backups ..... 10
Software sources ..... 11
Diskettes and other media ..... 11
Employee co-operation ..... 12
1.6 The Anti-Virus Toolkit ..... 12
FindVirus ..... 13
VirusGuard ..... 13
WinGuard ..... 13
ViVerify ..... 14
The Virus Encyclopedia ..... 14
More advanced features ..... 14

**2. Installing the Toolkit ..... 17**
2.1 Before you start ..... 17
2.2 How to install the Toolkit ..... 18
Installing the DOS Toolkit ..... 18
Installing the Windows and DOS Toolkit ..... 18
WinGuard ..... 20
VirusGuard ..... 20
Completion of installation ..... 23
2.3 Installing VirusGuard separately ..... 24
How VirusGuard uses memory ..... 24
Copying the VirusGuard files ..... 26
Running VirusGuard ..... 26
Using a RAM drive ..... 27
2.4 Creating a rescue diskette ..... 28
2.5 README files ..... 30
2.6 Upgrading the Toolkit ..... 31
To upgrade the DOS Toolkit ..... 31
To upgrade the Windows Toolkit ..... 32

**3. Finding your Way Around ..... 33**
3.1 Starting the Toolkit ..... 33
Starting from DOS ..... 33
Starting from Windows ..... 35
3.2 The main screen ..... 36
3.3 Options on the menus ..... 37
File menu ..... 37
Scan menu ..... 38
Repair menu ..... 38
Advanced menu ..... 39

**4. Guarding against Viruses ..... 41**
4.1 Using WinGuard ..... 42
Configuring WinGuard ..... 43
Advanced features of WinGuard ..... 46
If WinGuard reports a virus ..... 46
4.2 Using VirusGuard ..... 47
How VirusGuard uses memory under DOS ..... 47
If VirusGuard reports a virus ..... 48

**5. Checking for viruses ..... 51**
5.1 Finding viruses - FindVirus ..... 51
When to use FindVirus ..... 51
Running FindVirus from the main screen ..... 52
Running FindVirus from the user interface ..... 53
5.2 Checking for changes - ViVerify ..... 57
When to use ViVerify ..... 57
Running ViVerify ..... 58
Creating a file list ..... 59
Computing the fingerprints ..... 60
Checking the files ..... 61
If a file has changed ..... 61
Advanced menu options ..... 62
5.3 The Virus Encyclopedia ..... 65
5.4 Scheduling FindVirus and ViVerify ..... 67
To schedule FindVirus ..... 67
To schedule ViVerify ..... 68
Checking the schedules ..... 69

**6. If you Find a Virus ..... 71**
6.1 If VirusGuard or WinGuard report a virus ..... 71
What to do if VirusGuard or WinGuard sounds the alarm ..... 72
6.2 If FindVirus reports a virus ..... 73
What to do if FindVirus discovers a virus ..... 73
6.3 If ViVerify reports a changed file ..... 74
What to do if changed files are reported ..... 74
6.4 Single button repair ..... 75
6.5 If you discover a new virus ..... 76

**7. Advanced Virus Detection ..... 77**
7.1 How FindVirus works ..... 77
Heuristic Analysis ..... 78
Executable files ..... 79
Compressed and archived files ..... 79
Repairing files ..... 80
7.2 Running FindVirus from the user interface ..... 81

7.3 Running FindVirus from the command line ... 81
Scanning specific drives ... 81
Scanning files and subdirectories ... 83
Scanning boot and partition sectors ... 85
Producing reports ... 85
Specifying actions ... 86
Network options ... 87
Defining drivers ... 88
Repairing files ... 88
Heuristic Analysis ... 89
Requesting extended errorlevels ... 89
7.4 Hints and Tips ... 90
Errorlevels ... 90
Hard disk device drivers ... 91
Speeding up FindVirus ... 91
Scanning backup files ... 91
False alarms ... 92
Testing FindVirus ... 92
7.5 Error messages ... 92

**8. Advanced Virus Prevention ... 95**
8.1 How VirusGuard works ... 95
Requirements ... 95
Running VirusGuard ... 96
Use of memory ... 96
Security levels ... 97
Executable files ... 98
Boot sector scans ... 99
Finding viruses ... 99
8.2 Running VirusGuard ... 100
Scanning files when copying or reading ... 100
Scanning files when writing ... 101
Scanning Windows font files ... 102
Protecting diskettes ... 102
Location of virus driver ... 104
Changing the pop-up message ... 104
Using VirusGuard on a network ... 105
8.3 Hints and Tips ... 106
Changing the security level ... 106
Loading high ... 107
8.4 Testing VirusGuard ... 108
File virus test ... 108
Boot sector virus test ... 110
8.5 VirusGuard error messages ... 111
8.6 Marking diskettes with an authorization code ... 112

How Author works ..... 112
Running Author ..... 113

**9. Advanced Virus Checking ..... 115**
9.1 How ViVerify works ..... 115
Executable files ..... 115
Encryption algorithms ..... 116
Checking speed ..... 116
Running ViVerify ..... 117
9.2 Running ViVerify from the user interface ..... 117
9.3 Running ViVerify from the command line ..... 117
Checking specific drives ..... 118
Defining files to be checked ..... 118
Specifying a fingerprint file ..... 119
Excluding files ..... 120
Checking boot and partition sectors ..... 120
Specifying a keyword ..... 121
Varying the checking speed and security ..... 121
Specifying an algorithm ..... 122
Defining actions ..... 122
Producing reports ..... 122
Extended errorlevels ..... 123
Producing a list of suspect files ..... 123
Using anti-stealth measures ..... 124
Errorlevels ..... 124

**10. Additional Tools ..... 125**
10.1 Checking memory - GuardMem ..... 125
10.2 Examining disks - Inspect Disk ..... 126
Running Inspect disk from the user interface ..... 126
Running Inspect Disk from the command line ..... 129
10.3 Examining file contents - Inspect File ..... 129
10.4 Examining memory - Inspect Memory ..... 131
10.5 Anti-stealth measures ..... 132

**11. Virus Repair and Removal ..... 135**
11.1 Introduction ..... 135
11.2 Repairing drives ..... 136
Repairing drives from the user interface ..... 136
Repairing drives from the command line ..... 138
11.3 Replacing boot sectors ..... 139
How CleanBoot works ..... 139
Running CleanBoot from the user interface ..... 140
Running CleanBoot from the command line ..... 141
Cross-formatted diskettes ..... 142

11.4 Replacing partition sectors ..... 143
How CleanPart works ..... 143
Running CleanPart from the command line ..... 144
Backing up partition, boot and CMOS data ..... 144
Restoring partition and boot sector data ..... 145
Restoring CMOS data ..... 146
Replacing the hard disk boot sector ..... 147
Replacing partition sectors ..... 148
11.5 Shredding files ..... 150

**12. Using the Toolkit on a Network ..... 151**
12.1 Running VirusGuard on a network ..... 152
Use of memory ..... 152
Start-up order ..... 152
Maintaining VirusGuard centrally ..... 153
Network alarm messages ..... 154
Write checks on network drives ..... 155
Testing ..... 155
12.2 Running FindVirus on a network ..... 155
12.3 Anti-Stealth Methodology ..... 156
12.4 Dealing with infected networks ..... 156

**13. Toolkit Configuration ..... 159**
13.1 The TOOLKIT.INI file ..... 159
FindVirus ..... 160
FileRepair ..... 160
ViVerify ..... 161
13.2 The FINDVIRU.INI file ..... 161
13.3 Configuration File Management ..... 162
13.4 Toolkit security features ..... 163
To set or change a password ..... 164
To change settings ..... 165
To disable the security features ..... 165

**14. Toolkit Utilities ..... 167**
14.1 TKUTIL ..... 167
Reporting the disk drive ..... 168
Reporting the CPU ..... 169
Reporting memory type ..... 169
Reporting Toolkit TSRs ..... 170
Reporting the latest keystroke ..... 170
Reporting batch file run ..... 170
Make new directory ..... 171
Updating files ..... 171
Adding text to a file ..... 172

Deleting text from a file ....173
Searching for text ....174
Checking VirusGuard ....174
Checking RingFence ....175
Determining the day of the week ....175
Determining the day of the month ....176
Locking the PC ....176
Sounding an alarm ....176
Playing a tune ....176
Removing other anti-virus packages ....177
Send form feed to printer ....177
Restarting VirusGuard ....178
Restarting TSRs ....178
Reporting technical information ....178
14.2 Examples of batch files ....179
VIV1.BAT ....179
VIV2.BAT ....180
FRIDAY.BAT ....181
FV.BAT ....182

**15. Reference Information ....183**
15.1 TOOLKIT command ....183
Syntax ....183
Switches ....183
15.2 FINDVIRU command ....184
Syntax ....184
Switches ....184
15.3 GUARD command ....186
Syntax ....186
Switches ....186
15.4 VIVERIFY command ....187
Syntax ....187
Functions ....187
Switches ....187
15.5 CLEANPAR command ....189
Syntax ....189
Switches ....189
15.6 CLEANBOO command ....190
Syntax ....190
Switches ....190
15.7 WTKUTIL command ....191
Syntax ....191
Switches ....191
Commands ....191

**Glossary** ..... 193

**Index** ..... 203

# Preface

Dr. Solomon's Anti-Virus Toolkit contains everything you need to detect viruses on your PC, repair files and help prevent virus infection.

## How to use this manual

This manual includes information for anyone using the Anti-Virus Toolkit, from the non-technical user to the PC expert. The sections you are interested in will depend on your level of knowledge and the information you need to know.

Chapters 1 and 2 are important for all readers. They provide background information on viruses and explain how to install the Toolkit.

Chapters 3 to 6 cover how to use the user interface and explain in detail the most straightforward ways to search for viruses and repair infected files.

Chapters 7 to 15 are aimed at more technical users. Read these if you want more in-depth information; for example, if you want to configure the tools for your particular needs.

If you do not have time to read the whole manual, particularly if you think you have a virus, read the QuickStart pages at the front of this manual.

**Chapter 1 - Introduction** explains what computer viruses are and the damage they can do. It explains the resources available in the Anti-Virus Toolkit to prevent, detect and remove viruses.

**Chapter 2 - Installing the Toolkit** gives step-by-step instructions for installing the DOS and Windows versions of the Toolkit on your PC.

**Chapter 3 - Finding Your Way Around** shows you how to run the Toolkit programs, and explains the options that are available from each of the menus.

**Chapter 4 - Guarding against Viruses** describes the two memory-resident scanning programs that continually monitor disk and file accesses.

**Chapter 5 - Checking for Viruses** explains how to use the Toolkit to search for viruses on hard disks and diskettes.

**Chapter 6 - If You Find a Virus** outlines what happens if the Toolkit finds a virus. It explains the straightforward steps necessary to remove the virus and repair infections.

**Chapter 7 - Advanced Virus Detection** provides additional information on FindVirus, including running the program from the command line.

**Chapter 8 - Advanced Virus Prevention** gives detailed information on protecting your PC from virus infection using VirusGuard.

**Chapter 9 - Advanced Virus Checking** provides information on checking for changes in files using ViVerify.

**Chapter 10 - Additional Tools** includes information on the other programs in the Toolkit which you can use to protect your PC against viruses.

**Chapter 11 - Virus Repair and Removal** details the advanced options for repairing files, boot sectors and partition sectors. It also includes advice on removing viruses and preventing re-infection.

**Chapter 12 - Using the Toolkit on a Network** gives additional information if you are installing and running the Toolkit on a network.

**Chapter 13 - Toolkit Configuration** gives an explanation of the configuration files and how you can set them up and manage them.

**Chapter 14 - Toolkit Utilities** explains the various utilities provided in the Toolkit and how you can use them to create your own batch files.

**Chapter 15 - Reference Information** includes the definition and syntax of all Toolkit commands.

A glossary is provided at the end of the manual, covering all the important terms used. There is also a comprehensive subject index.

## Conventions

Throughout this manual, a number of conventions are used.

Information that you have to type is shown in the `Courier` typeface, for example:

```
COPY GUARD.COM C:\TOOLKIT
```

Keys that you have to press are shown in the following form:

is used to indicate the Return or Enter key.

Throughout the text, symbols appear in the margin to draw your attention to particular points. These are as follows:

This indicates a section or paragraph that applies only to the Windows version of the software.

This indicates a section or paragraph that applies only to the DOS version of the software.

This indicates important information or tips to which you should pay particular attention.

This indicates a warning, and you should read it carefully.

## What you need

The Toolkit runs on almost any PC. The basic configuration you need is:

- Any IBM or compatible PC (including XTs).
- DOS 3.1 or higher.
- Approximately 330 Kb of available memory.

This will enable you to run most of the Toolkit programs.

To install the DOS Toolkit on your hard disk, you need approximately 2.5 Mb disk space, while for the Windows and DOS Toolkit, you need approximately 5 Mb disk space.

If you wish to run VirusGuard, a memory-resident utility which scans continuously for viruses, it will run faster if your system has one of the following:

- Extended memory.
- Expanded memory.
- A RAM drive.

You also need a clean (that is, virus-free) write-protected DOS system diskette (boot diskette) to ensure that you start with a clean system. Ideally, you should use the boot diskette that was supplied with your PC or with the latest operating system upgrade.

If you want to run the Toolkit on a network, or on more than one PC at a time, you should enquire about a site license from S&S, or your international distributor if you are outside the UK.

## The Windows and DOS versions

This manual refers to both the DOS and Windows versions of the Toolkit. Almost all facilities and options are the same, although there are some minor variations in the screen displays.

Where features apply only to DOS or only to Windows, the appropriate symbol appears in the margin, for example:

The Toolbar feature is only available in the Windows version of the Toolkit.

Most of the screen representations in this manual show the Windows version.

If you have the Windows Toolkit, it includes the DOS version, as some of the Toolkit programs can only be run from DOS. The DOS Toolkit can be run from diskette as well as from the hard disk. Running from diskette is particularly useful if a virus infection prevents you from using the hard disk.

### Using a mouse

In both the Windows and DOS versions you can use a mouse to move around the screens and make selections. Since Windows was designed for use with a mouse, it is strongly recommended that you use a mouse if you run the Toolkit under Windows.

This manual assumes that you are familiar with the basic operation of the mouse, including how to point, click and drag. The left-hand mouse button is the primary one unless you have configured it otherwise.

## Using the keyboard

If you are using the Windows version of the Toolkit, a mouse is strongly recommended. If you are using the DOS version, use of a mouse is optional. However, all functions can be accessed from the keyboard if required.

Most menu options can be selected by pressing short-cut key combinations. In Windows, short-cut keys are underlined. In DOS they are indicated by red characters, reverse video, or bright characters, depending on the display mode.

Short-cut keys can always be used by pressing Alt + the short-cut key. For example, from the Toolkit user interface, pressing Alt + S displays the Scan drop-down menu.

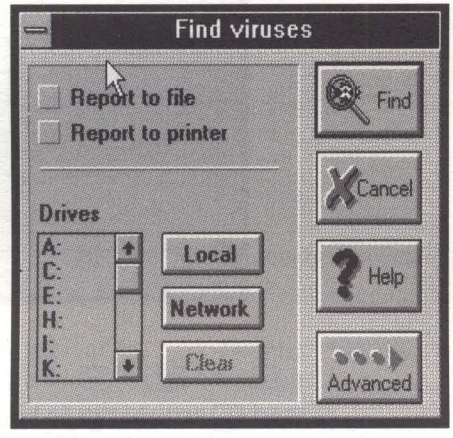
The following table explains the keys that can be used within the Toolkit:

| Key or combination | Function |
|---|---|
| ↵ | To accept a highlighted option button. The default button is usually OK. |
| Esc | To abandon an action and return to the previous screen. |
| Tab | To move to the next option in a dialog box. |
| Shift + Tab | To move to the previous option in a dialog box. |
| ↓ ↑ | Within a list of options, to move up and down the list. |
| Space | To select more than one option from a list. |
| F1 | To display a screen of help text relevant to what you are doing. |
| Pg dn | To scroll down within the help text. |

| Key or combination | Function |
|---|---|
| Pg up | To scroll up within the help text. |

## Dialog boxes

For some menu options, you need to enter information in a dialog box. For example, if you select Find Viruses from the Scan menu, the following window is displayed:




Press Tab to move between the various boxes or options.

Press Shift + Tab to move backwards between the various options.

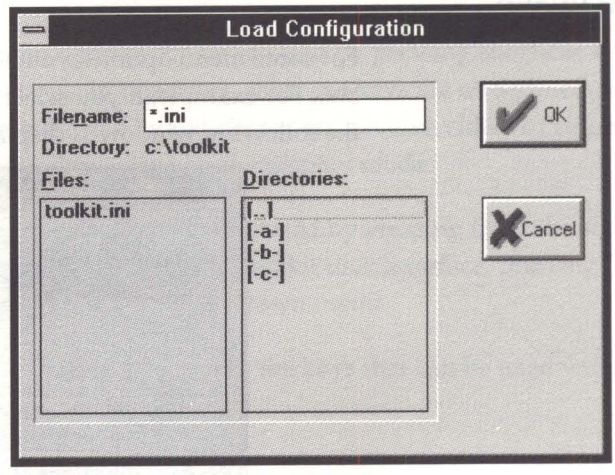
Use the ↓ and ↑ to select items from a list. Alternatively, you can press the highlighted letter to select an option. For example, on the above example, press A, B or C to select the disk drive to be checked.

In cases where you can select several options from a list, such as the Drives box above, move to the required item, then press the space bar to select or deselect it.

When all the selections are set correctly, press ↵ or select the option required to run the option.

## File selection

In some options, you need to enter or select a file before going any further. In these cases a file selection box is displayed as follows:



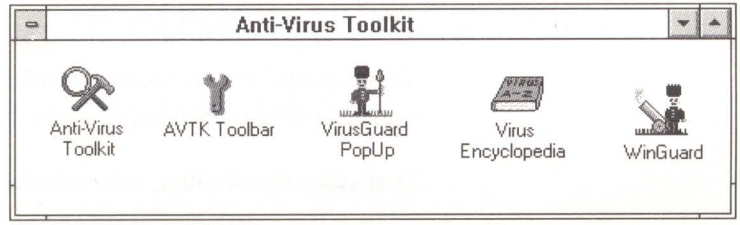

Use Tab and Shift + Tab to move to each box in turn, then use the ↓ and ↑ arrow keys to highlight the appropriate item. Press ↵ when you have selected an item.

For example, in the above file selection box, press Tab to move to the Directories box, select the appropriate directory, then press ↵ to display a list of files and subdirectories in this directory.

To enter a filename, just type it in the Filename box, overwriting any previous contents.

## Windows icons

The icons in the Anti-Virus Toolkit are as follows:




| Item | Purpose |
|---|---|
| Anti-Virus Toolkit | Starts the Toolkit and displays the user interface. |
| AVTK Toolbar | Displays the Windows Toolbar. See "Windows Toolbar" on page xxiv. |
| VirusGuard Pop-up | Ensures that the VirusGuard pop-up alarm box is displayed if a virus is detected while Windows is running. |
| Virus Encylopedia | Displays the Virus Encyclopedia directly, enabling you to search for a particular virus. |
| WinGuard | Displays the WinGuard user interface. |

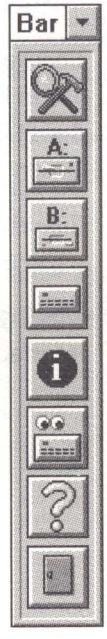
## Windows Toolbar

The Toolbar is a way of displaying the Toolkit options on the screen at any time you are running other Windows applications. It takes up less space than the main menu screen, but means all the short-cut options are available.

This is useful if you need to check frequently for viruses, for example, if you are using a lot of different diskettes.

To display the Toolbar, select the icon:

The bar appears on the screen as shown below:




Displays the Toolkit menu screen.

Checks drive A for viruses, using FindVirus.

Checks drive B for viruses, using FindVirus.

Checks all local drives for viruses, using FindVirus.

Displays the Virus Encyclopedia.

Runs Inspect Disk to display the contents of a disk.

Displays help text.

Closes the Toolbar window.

The toolbar can be minimised in the usual way.

Options are available to change the way the Toolbar is displayed.

1. Select Run from the File menu.
2. In the Command Line, enter the command:

   ```
   C:\TOOLKIT\BAR.EXE
   ```

   with one of the following switches:

| | |
|---|---|
| `/HORIZ` | Displays the Toolbar horizontally instead of vertically. |
| `/BLOCK` | Displays the Toolbar as a rectangular block of icons rather than as a strip. |
| `/HIDE` | Prevents the Toolbar from being displayed in front of any other windows. |

For example:

```
C:TOOLKIT\BAR.EXE /BLOCK /HIDE
```

would display the toolbar as a block of icons, and it would not appear in front of any other open windows.

## On-line help

On-line help information is available in both the DOS and Windows versions.

Select Help from the Toolkit menu to display a drop-down menu of help information. The items available on this menu are as follows:

| Menu item | Function |
|---|---|
| Index | Displays an alphabetic list of help topics available. You can scroll through the list or search for a particular topic. |
| Using help | Explains how to find your way through the help system. |
| Keyboard | Explains how to choose options and make selections using the keyboard. |
| Procedures | Displays a reminder of what to do if you find a virus. |
| Virus-L FAQ | Answers a number of frequently-asked questions about viruses. This is only available in the Windows version. |

The Help text contains cross-references, highlighted in a different colour. You can select these to jump to additional topics.

While you are using the Toolkit, you can also display help text relevant to your current activity by pressing F1 or by selecting the Help button within a dialog box.

# Related documentation

## The Virus Encyclopedia

Included with your Toolkit is a copy of the Virus Encyclopedia book. As well as giving background information about viruses, it includes details of many of the viruses that the Toolkit can detect. The Encyclopedia categorizes each virus, describes its effects and explains how it can be removed. It also lists any alternative names by which the virus is known.

An on-line version of the Virus Encyclopedia is also included in the Toolkit. As new viruses are found, they are included in the latest Toolkit upgrade. It is therefore possible for details of new viruses to be included in an upgraded version of the on-line Encyclopedia but not in the printed copy.

## Other versions of the Toolkit

### Novell NetWare

The NetWare version of the Toolkit provides tools to protect NetWare servers and workstations from viruses. For complete protection, the package also includes the Windows and DOS version of the Toolkit.

### OS/2

There are now specific viruses which can infect OS/2 systems. The Anti-Virus Toolkit for OS/2 provides full protection for OS/2 systems, detecting OS/2, DOS and Windows viruses. The package also includes the full DOS version of the Toolkit.

### Windows 95

The Windows 95 version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for all PCs running Windows 95. The package also includes the full DOS version of the Toolkit.

### Windows NT

The Windows NT version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for all Intel-based PCs running Windows NT. The package also includes the full DOS version of the Toolkit.

### SCO UNIX

The SCO UNIX version of the Anti-Virus Toolkit provides virus detection, repair and protection facilities for PCs running SCO UNIX. The package includes the DOS version of the Toolkit.

### Apple Macintosh

At the time of writing, a version of the Anti-Virus Toolkit is in preparation for Apple Macintosh. For more information, contact S&S or your authorized distributor.

## Registration and upgrades

You will find a user registration card inside the Toolkit license envelope. Complete the details on the card and return it to S&S or the representative in your country. If you do not register your purchase you will not receive upgrades to the Toolkit.

If you cannot find the registration card, call S&S or the representative in your country and quote the serial number on the Installation Disk.

The virus researchers at S&S constantly receive specimens of new viruses for investigation, and the Toolkit is upgraded each month to take account of these. Typically, between 100 and 150 new viruses are reported every month. If your Toolkit is out-of-date, a message appears on the screen when you run the software, to remind you to upgrade.

For your own protection you should therefore subscribe to the regular software upgrade service. For many people, a quarterly upgrade offers sufficient protection, but if your system is at particular risk or if security is of major importance, monthly upgrades are also available.

Your Toolkit comes with a pre-paid subscription for the first year of upgrades. Once you register you will automatically be sent monthly or quarterly upgrades for 12 months from the date on the card.

If you don't send us the card, you will not receive the upgrades that you have already paid for.

Send in your registration card.

# If you need help

If you have a problem while installing or running the Toolkit, there are a number of ways in which you can obtain help.

Check the documentation carefully, including any README files on the disks as well as this manual and the help text. Make sure you have installed the software correctly. Your authorized distributor may also be able to advise you.

If you still cannot solve the problem, S&S support staff are available to help you. This service is free of charge.

You can contact S&S by any of the following methods:

**UK Office**

| | |
|---|---|
| By telephone: | +44 (0)1296 318700 |
| By fax: | +44 (0)1296 318734 |
| By e-mail: | support@drsolomon.com |
| By bulletin board: | +44 (0)1296 318810 |
| By post: | S&S International PLC<br>Alton House<br>Gatehouse Way<br>Aylesbury<br>Buckinghamshire<br>HP19 3XU<br>United Kingdom |

**US Office**

| | |
|---|---|
| By telephone: | +1 617 273 7400 |
| By fax: | +1 617 273 7474 |
| By e-mail: | support@us.drsolomon.com |
| By bulletin board: | +1 617 229 8804 |
| By post: | S&S Software International, Inc.<br>17 New England Executive Park<br>Burlington<br>MA 01803<br>USA |

**German Office**

| | |
|---|---|
| By telephone: | +49 (0)40 2519 54-0 |
| By fax: | +49 (0)40 2519 54-50 |
| By e-mail: | support@de.drsolomon.com |
| By post: | S&S International (Deutschland) GmbH<br>Luisenweg 40<br>20537 Hamburg<br>Deutschland |

**World Wide**

| | |
|---|---|
| CompuServe: | GO DRSOLOMON |
| World Wide Web: | http://www.drsolomon.com/ |

When you contact S&S, it is helpful to have the following information available:

- Your name and company.
- Your serial number as printed on the Installation Disk.
- The version of DOS you are using (you can find this out by typing VER at the DOS command line).
- The version of Windows you are running, if applicable.
- The version number of the Toolkit you are using (this is printed on the label of the diskettes).
- In the case of an application error, any error messages reported.

If possible, you should be at the particular PC when you call us. We may need additional information, or we may ask you to carry out some diagnostic tests.

# 1. Introduction

Computer viruses are a growing problem. When S&S published the first version of the Anti-Virus Toolkit in 1989, the number of viruses at large in the world was in single figures. A year later, there were 50, and in the following year there were 200. By November 1995 there were over 7000. Between 100 and 150 new viruses are reported each month.

Many people panic when they hear the word *virus*. Remember though, computer viruses can be prevented, and if a virus infection is caught early it need not be particularly disruptive. The more preventative measures you can take the better, but you also need to be able to deal with a virus outbreak.

Dr. Solomon's Anti-Virus Toolkit will help prevent viruses and deal with virus infections. It provides you with several levels of protection against attack by viruses, and detects and removes any known virus.

This manual also gives you some useful guidelines for establishing an anti-virus policy and for dealing with an outbreak, should one occur.

## 1.1 What is a virus?

Computer viruses are so-called because they copy themselves. There are other types of software that can cause problems on your PC, and some of these are discussed in "Other potential problems" on page 7. However, no other type of software can replicate and it is this characteristic which makes a program a virus.

A virus is designed to copy itself without your knowledge. For example, it may attach itself to the DOS program FORMAT and run every time you format a diskette.

If viruses do nothing but copy themselves, why are they such a problem?

Firstly, most viruses have deliberate or accidental side effects. Some of these seem harmless - they may display a message, make letters fall from the screen or play a tune. Others are specifically designed to be destructive, overwriting selected data or deleting files from the hard disk. In addition, many viruses do not operate as their authors intended them to because of bugs in the software; the side effects of these viruses are unpredictable. From the user's point of view, it does not matter whether the damage caused by a virus was a deliberate act by the virus author or an error in the program.

Secondly, most viruses stay in your PC's memory where they can cause problems by interfering with other software you are trying to run.

Thirdly, once you have a virus, it is very likely that you will unwittingly pass it on to a colleague or a customer, who may well lose confidence in you and your company.

No virus is completely harmless; they all waste your time, processor time, memory and disk space. Dr. Solomon's Anti-Virus Toolkit can help ensure that your PC remains free from such disruption and from virus infection.

## 1.2 Types of virus

### File viruses

File viruses infect executable program files; these may include some data files containing executable macros. These usually, but not always, have COM or EXE file extensions. When you run an infected program the virus runs first, then passes control to the original program. While it has control, the virus code copies itself to another file or to another disk, replicating itself.

The majority of file viruses are memory-resident. This means that after the virus program has finished running, it remains in memory. (These programs are also known as TSR, or Terminate and Stay Resident programs.) Once in memory, the virus infects every program that is subsequently run. It can also interfere, deliberately or accidentally, with the operation of other memory-resident programs. Some TSR viruses infect other programs when they are opened or copied as well as when they are run. These are known as *fast infectors*.

A few viruses do not load into memory. Instead, when the infected program is run, they look for another program to infect.

## Macro viruses

There are now macro viruses in existence, for example, the Concept virus that infects Word 6 document files. This virus can infect Word 6 on any operating system including Windows. Many applications now have similar macro languages which could potentially be used to create viruses in the future.

## Boot and partition sector viruses

The boot sector is the part of every hard disk and diskette which is read by the computer when it starts up. The boot sector of a system disk contains the code necessary to load the DOS system files; a data disk contains the code necessary to display the message that the PC cannot be booted from that disk.

The partition sector is the first part of a hard disk to be read after the system has started up. It contains information about the disk such as the number of sectors in each partition and the location of all the partitions. The partition sector is also called the Master Boot Record (MBR).

Most PCs are set up to attempt to boot from the A: drive first. If the boot sector of a diskette is infected, the virus runs when you attempt to boot from the diskette. For example, if you leave a diskette in the drive overnight and then switch on your PC the next day, the following message, or similar, is displayed:

```
Non-system disk or disk error
Replace and press any key when ready
```

If the diskette is infected with a boot sector virus, that virus has already run, and your PC may already be infected.

In most cases, the virus loads itself into memory and infects the partition sector of the hard disk. It moves the partition sector elsewhere on the disk, and replaces the original partition sector with its own code. Some viruses also infect the boot sector of the hard disk.

If the partition sector is infected, when the PC is rebooted from the hard disk, the virus is loaded into memory. Any diskette subsequently accessed is infected. The virus moves the boot sector elsewhere on the diskette, and replaces the original boot sector with its own code.

Boot and partition sector viruses are the most common type of virus and are very easily spread. They can infect any PC, regardless of the operating system, since the virus runs before the system starts up.

## Companion viruses

If you have a COM file and an EXE file of the same name, DOS always runs the COM file in preference to the EXE file if no file extension is given. Companion viruses make use of this fact by creating COM files with the same name as the legitimate EXE files, thus ensuring they are executed. They then pass control to the original EXE file which runs normally.

### Overwriting viruses

An overwriting virus simply overwrites each file it infects with itself, so the program no longer functions. Since this is very easy to spot these viruses do not spread very well, and are not a real threat.

### Multipartite viruses

Some viruses use a combination of techniques to spread, and infect executable files, boot sectors and partition sectors.

### Droppers

A dropper is a program, not a virus itself, that installs a virus on the PC while performing another function.

## 1.3 Characteristics of viruses

### Stealth

Although some virus infections are readily apparent to the user, the most successful viruses try to remain as inconspicuous as possible so that they can spread without being noticed. A virus which uses *stealth* is one that tries to conceal its presence on the disk so that everything appears to be running normally. Many boot sector viruses use a certain amount of stealth; after running they pass control to the original boot sector so that the PC starts up normally. A detailed discussion of stealth, and ways to counteract it, is given in the Virus Encyclopedia. The Toolkit has extensive anti-stealth capabilities built in to it.

### Polymorphism

Many virus detection programs work by looking for a known pattern of bytes in the code of the virus. A *polymorphic* virus is one that tries to avoid detection in this way by ensuring that its code does not have a fixed pattern of characters. Usually the virus achieves this by encrypting itself differently each time it runs.

The Toolkit can deal effectively with polymorphic viruses using the Generic Decryption Engine. This can decrypt the virus without knowing the encryption method, allowing virus-scanning software to identify the virus and repair the infected files. It achieves this extremely rapidly and without any time-wasting false alarms. The Generic Decryption Engine is built into the Toolkit's main scanner, FindVirus.

More information on polymorphic viruses is given in the Virus Encyclopedia.

## Virus names

Many viruses appear to have several different names. This happens because most viruses are named by the anti-virus researchers who identify them, rather than by their authors, who prefer to remain anonymous. Different researchers often give viruses different names, based on text within the virus code or where they were first discovered.

S&S uses names which are approved by the Computer Anti-Virus Researchers Organisation (CARO). In addition, the Virus Encyclopedia lists any aliases by which the virus is commonly known.

## Variants

Many viruses are found in a number of related variations, often because their authors have simply amended the code of existing viruses. The Virus Encyclopedia includes details of many known variants which the Toolkit is able to find and deal with.

## How viruses spread

The most common way in which a virus is spread is via an infected diskette. Boot sector viruses are the most common type of virus, and they can only be transmitted by a diskette. People who use diskettes on a number of different PCs increase their chances of picking up an infected diskette and spreading the virus.

Some people mistakenly assume that shareware, free disks and games are the only sources of viruses. Although viruses are sometimes transmitted through these types of software, because they tend to be copied more, they have also been found in shrink-wrapped software distributed by major companies, and on diskettes accompanying hardware. For this reason, you should always scan all diskettes for viruses before they are used.

File viruses can also be spread by downloading infected programs from bulletin boards. You should take care to check any software transferred over a network or communications link before using it.

A workstation on a network can be infected in the same way as a standalone PC, and a virus can spread very quickly across a network. Since the effect of a virus infection can be particularly serious if a file server becomes infected, you should take particular care to protect PCs connected to networks from infection.

## 1.4 Other potential problems

When something goes wrong with a PC, it is easy to think it must be a virus. Unfortunately, there are many other problems which can disrupt work and destroy data. Some of these are described below.

### Bugs

A bug is an unintentional fault in a program. Virtually all complex software contains bugs. Minor bugs merely cause inconvenience, while major bugs can cause catastrophic data loss. There is no way of detecting bugs, and the only defense is to ensure you back up your important data regularly.

## Low-level software clashes

Low-level programs are those which work on disks directly. They are so-called because they function below the level of the operating system, which normally controls access to disks and enforces certain rules. Low-level programs include:

- Disk sector editors.
- Disk caching programs.
- Disk compression software.
- Defragmenters.

These tools are usually quite safe to use if you only run one at a time, but problems can occur if you run two or more low-level tools at the same time. If two or more tools try to access the disk, potentially dangerous clashes can result. As these tools become more common, this type of problem is more and more likely to occur.

To avoid problems with low-level tools:

- Always take a backup before using any disk utilities.
- Do not run more than one utility at the same time.
- Avoid using these tools at the same time as using memory-resident software.
- Always read the manuals and any README files supplied with the product. If the manufacturer has included any special warnings, there is usually a good reason for them!

## Trojans

Trojans are programs which do something unexpected and usually damaging. They are less widespread than viruses because they do not replicate, but they can represent a threat when copied. Many people confuse the two - the AIDS Information Diskette, often cited by the media as an example of a virus, was actually a trojan. Also, viruses sometimes contain trojans.

You are unlikely to encounter a trojan if you always obtain your software from reputable sources, but the main defense against damage by such programs is to back up your system.

The Toolkit finds and identifies some known trojans and treats them in the same way as viruses.

## Time bombs and logic bombs

These are particular types of trojan. A time bomb is set off on a particular date, while a logic bomb is triggered by a specific set of conditions, such as the number of files on a disk or a certain sequence of characters being entered. Both types usually do something damaging.

## Jokes

Some programs claim to be doing something destructive to your computer, but are actually harmless jokes. For example, a message may appear suggesting that your hard disk is about to be reformatted. Unfortunately, it is easy to over-react to the joke and cause more damage by trying to eradicate something that is not, in fact, a virus.

The Toolkit finds and identifies a number of widespread joke programs, and treats them in the same way as viruses.

## Human Error

When something goes wrong with your PC, or you lose data, the most likely cause is not a virus or a software problem, but human error. Everybody makes mistakes such as pressing the wrong key sequence or typing DEL *.* in the wrong directory, and these can have drastic results.

Remember that the most valuable part of your computer is the data you have stored on it. Hardware and programs can be replaced but you can only replace your data if you have backed it up.

## 1.5 What you can do

The data recovery specialists at S&S see a lot of people who have lost their data. Fortunately, the data can nearly always be restored and we can usually identify the reason that it was lost in the first place.

Although viruses are a problem, the scale of the problem should be kept in perspective. The most common reason for losing data is human error. The second most common cause is hardware failure, followed by software problems and bugs. Viruses come a poor fourth.

However, implementing a straightforward anti-virus policy will help protect your data from all kinds of loss, including viruses. In particular, you should consider the following three elements of protection:

- **Prevention** - to ensure that a virus does not get on to your PC in the first place.
- **Detection** - to ensure that if a virus does get through the defenses, it is discovered as quickly as possible.
- **Recovery** - to ensure that if any files are lost or damaged, they can be restored as quickly as possible.

Using the Anti-Virus Toolkit is obviously a significant part of the policy, but some other elements of a sensible anti-virus policy are suggested below.

### Backups

The most important precaution you can take against any kind of data loss is to make regular backups of your system. This cannot be stated too often! If you do not back up your data regularly, it is at risk.

Remember to check your backups frequently and make sure that you can restore your data from them.

Check that you have clean copies of all your executable files on diskette. All your backup diskettes and your boot diskettes should be write-protected.

## Software sources

Make sure that all your software comes from a reputable source. Check that software is in its original packaging.

Never use pirated software. Even if you feel entitled to use another copy temporarily (for example, because you left your licensed copy at another site) remember that the copy may expose you to virus infection.

Software can enter your PC via the communications ports as well as via portable media. Take care when transferring software to and from laptops and across networks and when downloading files from bulletin boards.

## Diskettes and other media

The risk of virus infection via diskette is particularly high, but you can take some simple steps to increase security.

- Keep diskettes write-protected wherever possible, to prevent viruses being copied.
- Do not leave diskettes in the drive when you turn off the PC. This will prevent you accidentally trying to boot from a diskette infected with a boot sector virus.
- If you do accidentally boot from a non-bootable diskette, switch off and start again instead of proceeding with the boot from the C: drive.
- Change the CMOS setting of your PC so it boots from the C: drive first rather than the A: drive.
- Use alternative methods of file transfer where possible.
- Remember that files on tape may have been infected when the back-up was made.

### Employee co-operation

You need the willing co-operation of your employees in any anti-virus policy. If members of staff think that they are likely to be disciplined if they discover a virus, they are unlikely to report any problems.

Some companies have attempted to ban the playing of games. It is much a better policy to ensure that games come from a reputable source and are checked before use. It can be useful to give one person or a small group the responsibility of checking and distributing games software.

## 1.6 The Anti-Virus Toolkit

The Anti-Virus Toolkit provides a set of tools for the prevention, detection and removal of viruses.

There are two major types of anti-virus software.

- A *scanner* is a program that searches files or PC memory for known viruses. Since new viruses are always appearing, scanners need to be updated regularly.

- A *checksummer* detects changes in files. It calculates a unique numeric fingerprint, known as a checksum, for each file to be protected. The checksummer can then be run to re-calculate this fingerprint to monitor any differences. Executable files do not usually change, so if there is a difference in the fingerprint, a virus may be present.

Dr. Solomon's Anti-Virus Toolkit includes both scanners and checksummers, as well as tools to repair infection. The various tools are described below.

## FindVirus

FindVirus is a scanner which you can use regularly to scan your hard disks and any incoming diskettes. It will find and report any known virus, that is, one held in the current version of the driver file. It also includes an optional heuristic scanner which looks inside files for suspicious code that may indicate a previously unknown virus.

FindVirus will find viruses in files, boot sectors, partition sectors and memory. It can also be used to repair virus infections. FindVirus can be used to scan incoming diskettes and files on a sheep-dip PC - one that is always used for that purpose. FindVirus scans very quickly and can be used for scanning hard disks on a daily basis.

## VirusGuard

VirusGuard is a memory-resident scanner which scans continuously for viruses. It identifies known viruses and prevents access to any file if a virus is found. VirusGuard detects virtually all the viruses in the current driver file. However there are a few particularly complex polymorphic viruses, which VirusGuard can detect but cannot prevent from running.

## WinGuard

WinGuard is a Windows memory-resident scanner (VxD) which takes over from VirusGuard when Windows in run. When both VirusGuard and WinGuard are enabled (as recommended), then control is passed automatically between them as Windows is started up or shut down.

Using Windows technology, WinGuard is able to detect all known viruses, including complex polymorphic, quickly and accurately.

WinGuard for Windows3.x will not work with Windows 95 or Windows NT. A version is available for Windows 95.

## ViVerify

ViVerify is a checksummer which detects changes in executable files that may have been caused by a virus infection. Initially you can use ViVerify to calculate a fingerprint, or checksum, for each file. You can then run ViVerify regularly to re-calculate this fingerprint and check if there are any changes. Although a change to an executable file does not necessarily mean that the file is infected, executable code does not normally change. ViVerify reports any possible virus, even a previously undiscovered one.

## The Virus Encyclopedia

The on-line Virus Encyclopedia includes details of the most common viruses which the Toolkit can detect, including any variants. The on-line Virus Encyclopedia is more comprehensive than the Encyclopedia manual.

## More advanced features

The Toolkit includes a number of other programs for detecting viruses and investigating problems:

### GuardMem

This program scans memory and reports the presence of any known memory-resident viruses.

### Author

Author is a program which allows you to mark diskettes with an authorization code. You can then use VirusGuard to check diskettes for the correct code as well as for viruses. This helps if you want to prevent unauthorized diskettes from being used on your PC.

### Inspect Disk

Inspect Disk enables you to examine hard disks and diskettes for suspect code.

### Inspect File

Inspect File allows you to look at the contents of a file in both ASCII and hexadecimal.

### Inspect Memory

Inspect Memory allows you to examine the contents of memory in both ASCII and hexadecimal.

### CleanBoot

CleanBoot replaces an infected boot sector on a diskette with a new, non-infected boot sector.

### CleanPart

CleanPart is a diagnostic and repair program which repairs partition sectors and hard disk boot sectors which have been moved or corrupted by a virus.

### Shred

This facility deletes files in such a way that they cannot be restored by file recovery programs.

# 2. Installing the Toolkit

This chapter explains how to install the DOS and Windows versions of the Toolkit on your PC, and how to create a rescue diskette which can help you repair virus infection.

## 2.1 Before you start

You can either run the Toolkit from a diskette or you can install it on the hard disk and run it from there. Running it from a clean write-protected diskette provides more security, as you can be sure that the diskette is free from viruses before you start. Additionally, if a virus infection has damaged files on your hard disk, you may find you have to run the Toolkit from diskette. However, in normal use you may find it more convenient to keep the programs constantly accessible on the hard disk.

If you intend to use VirusGuard to scan constantly for viruses it must be installed on your PC, since it is memory-resident and cannot be run in any other way.

Before you start, decide exactly what you want to install:

- If you want to install the entire Toolkit on your hard disk, you should read "How to install the Toolkit" on page 18.
- If you intend to run the Toolkit from diskette, and you just want to install VirusGuard, see "Installing VirusGuard separately" on page 24.

This chapter also explains how you can create a rescue diskette, which will help recovery if you have a virus infection. For details, see "Creating a rescue diskette" on page 28.

Before using the Toolkit, you should make a copy of the program disks as a backup. Note that the terms of your license agreement allow you to make one copy only.

## 2.2 How to install the Toolkit

To install the Toolkit, follow the steps given below for either the DOS or the Windows version.

Installing the Windows version also installs the DOS files, since some Toolkit programs must be run under DOS.

### Installing the DOS Toolkit

1. Boot the PC from a clean, write-protected DOS system diskette.
2. Insert the diskette labelled Installation Disk 1 of the DOS Anti-Virus Toolkit into the A: drive.
3. Change to that drive by typing `A:` and press ↵.
4. At the `A:` prompt, type `INSTALL` and press ↵.

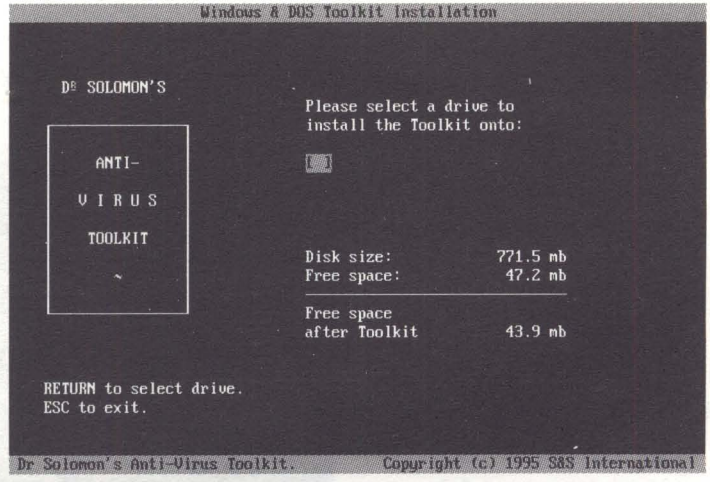
Go to step 5 below.

### Installing the Windows and DOS Toolkit

The Windows Toolkit must be installed from DOS:

1. Boot the PC from a clean, write-protected DOS system diskette.
2. Insert the diskette labelled Installation Disk 1 of the Windows Anti-Virus Toolkit into the A: drive.
3. Change to that drive by typing `A:` and press ↵.
4. At the `A:` prompt, type `SETUP` and press ↵.

5. Whichever version you are installing, the following screen is displayed:




6. This screen allows you to check how much space you have available on your hard disk. The DOS Toolkit requires approximately 2.5 Mb, and the Windows Toolkit takes up approximately 5 Mb. If you do not have enough space on your hard disk, quit the installation process by pressing Esc. Check if there are any files you can delete to make room.

7. The Toolkit is installed on the C drive unless you specify otherwise. Select an alternative disk drive if required and press ↵.

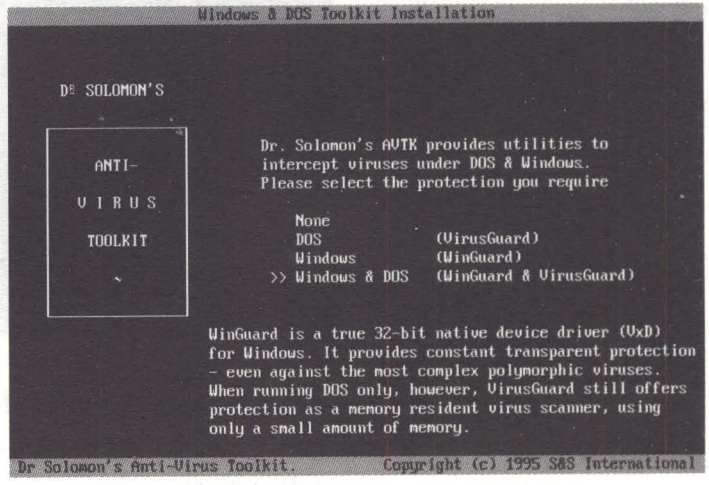
8. You are then asked to specify an installation directory. This is called TOOLKIT unless you specify an alternative name. Press ↵.

9. The installation process then starts.

You are prompted to insert further disks during the installation process. You can cancel the installation at any time by pressing Esc. If you then want to re-install, you should delete any files in the Toolkit directory that were created in the original installation.

When the main Toolkit files have been installed, you will be prompted to enable installation of either or both of VirusGuard and WinGuard. You are strongly recommended to enable both WinGuard and VirusGuard.

The following screen is displayed:


Windows & DOS Toolkit Installation
Dr SOLOMON'S
ANTI-
VIRUS
TOOLKIT
Dr. Solomon's AVTK provides utilities to
intercept viruses under DOS & Windows.
Please select the protection you require
None
DOS (VirusGuard)
Windows (WinGuard)
>> Windows & DOS (WinGuard & VirusGuard)
WinGuard is a true 32-bit native device driver (VxD)
for Windows. It provides constant transparent protection
- even against the most complex polymorphic viruses.
When running DOS only, however, VirusGuard still offers
protection as a memory resident virus scanner, using
only a small amount of memory.
Dr Solomon's Anti-Virus Toolkit.
Copyright (c) 1995 S&S International

## WinGuard

WinGuard is a memory-resident program which runs under Windows. It checks that files and disks are free from infection before permitting access to them.

The install process copies files from the disks and adds necessary lines to the Windows system files.

On-screen help is available if you need more information, and further details are also given in Chapter 4 "Guarding against Viruses" in this manual.

## VirusGuard

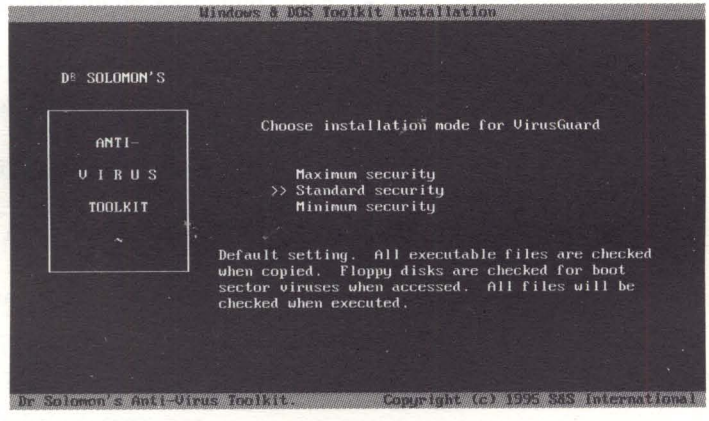
VirusGuard is the Toolkit's DOS memory-resident program, which scans continuously for viruses. It is an optional part of the installation as on some older PCs it can affect system performance.

If your PC has either extended or expanded memory, you are recommended to install VirusGuard. If you do not have additional memory, VirusGuard can run from the hard disk but it will be slower. If you are using an XT, you may notice that the PC runs more slowly. See Chapter 8, "Advanced Virus Prevention" for information on configuring VirusGuard and optimizing its performance.

If you don't install VirusGuard now, you can install it separately later. See "Installing VirusGuard separately" on page 24.

If you install VirusGuard, the system may require changes to the AUTOEXEC.BAT and CONFIG.SYS files. In this case, copies of the original files are made and saved in the root directory of the specified hard disk. The names of the backup files created are displayed on the screen; you may wish to make a note of them. (For more information, see Chapter 8, "Advanced Virus Prevention".)

After you have selected the required virus protection, the following screen is displayed:


Windows & DOS Toolkit Installation
Dr SOLOMON'S
ANTI-
VIRUS
TOOLKIT
Choose installation mode for VirusGuard
Maximum security
>> Standard security
Minimum security
Default setting. All executable files are checked when copied. Floppy disks are checked for boot sector viruses when accessed. All files will be checked when executed.
Dr Solomon's Anti-Virus Toolkit.
Copyright (c) 1995 S&S International

You can choose to run VirusGuard in any one of three security levels. Use the ↓ and ↑ keys to select the option you want, then press ↵.

**Maximum security**
In maximum security mode, VirusGuard will scan the following:

- All diskettes for boot sector viruses.
- All files that are copied.
- All files that are written to disk.
- Executable files when they are run.

This option offers the greatest security, but the extent of the checking is likely to reduce system performance.

**Standard security**
This is the default installation mode, and the one that is recommended for most users. In this mode, VirusGuard scans the following:

- All diskettes for boot sector viruses.
- Executable files that are copied.
- Executable files when they are run.

**Minimum security**
With this option set, VirusGuard only scans the following:

- All diskettes for boot sector viruses.
- Executable files copied from diskette.
- Executable files when they are run.

In all cases, when scanning executable files, VirusGuard looks for files with the following extensions:

| | |
|---|---|
| APP | EXE |
| BIN | OVL |
| COM | OVR |
| DLL | SCR |
| DOC | SYS |
| DOT | XTP |
| EXE | |

You can also optionally check files with the FON extension (see "Scanning Windows font files" on page 102).

If you are unsure of the security level to choose, select the default setting of standard security. You can change it later if you wish (see "Changing the security level" on page 106).

## Completion of installation

When the installation process is complete, FindVirus runs automatically to scan for any viruses. If a virus is reported, refer to Chapter 6, "If You Find a Virus" for information about what to do.

The installation is now complete, and your PC has been scanned for viruses. Press any key to return to the DOS prompt.

If the screen reports a virus on your PC, do not panic! See Chapter 6, "If You Find a Virus", for information about what to do.

If you have problems installing the Toolkit, check that you have followed the procedure in this manual. If you cannot resolve the problem, contact S&S Technical Support. See "If you need help" on page xxx.

## 2.3 Installing VirusGuard separately

VirusGuard provides the Toolkit's DOS memory-resident virus monitoring system. If you have installed VirusGuard as part of the Toolkit, as explained in "How to install the Toolkit" on page 18, you need not read this section.

If you intend to run the Toolkit from diskette, and therefore have not installed VirusGuard on your hard disk, it is recommended that you install VirusGuard separately by copying the relevant files on to your hard disk.

VirusGuard consists of three files:

```
GUARD.COM
GUARD.DRV
MESSAGES.DRV
```

To run VirusGuard, you need to make sure that the files are installed and then run the VirusGuard program. If you have not installed the Toolkit on the hard disk, you will have to create a suitable directory. This manual suggests that you use a directory called TOOLKIT.

### How VirusGuard uses memory

Most PCs have up to 640 Kb of conventional memory, which is used to run DOS and the standard device drivers and commands. However, VirusGuard, like many other programs, works faster if your PC has additional resources in the form of extended or expanded memory.

Extended memory (XMS) is only available on PCs with 286 or higher processors. If you are running Windows 3.0 or later, your system will almost certainly have extended memory.

Expanded memory (EMS) was an earlier form of additional memory and is more common on older PCs. It only allows programs to access a limited amount of information at a time, and can be slower than extended memory.

If you are unsure of the type or amount of memory your PC has, you can find out by typing the DOS command MEM at the system prompt.

If you have expanded or extended memory, VirusGuard automatically uses the most appropriate memory option when it runs. It checks for extended memory first, and if this is not present, or if there is not enough contiguous extended memory available, it looks for expanded memory.

Some computers which do not have extended or expanded memory have memory that can be used as a RAM drive. In this case you can set up VirusGuard to use the RAM drive, which is nearly as fast as using extended or expanded memory. Details are given in "Using a RAM drive" on page 27.

If you have an older computer which does not have extended or expanded memory, and you do not have a RAM drive, VirusGuard has to access the virus driver file from the hard disk. This is considerably slower than using memory, and you will notice some degradation in performance.

If your PC is on a network, it is possible to run VirusGuard from a network drive. This is not recommended if you have an alternative, as it can slow down system performance. For more information, see Chapter 11, "Using the Toolkit on a Network".

## Copying the VirusGuard files

You need to copy the VirusGuard files from the Toolkit diskette to your hard disk.

If you have already installed the Toolkit, even if you have specified that you do not want to use VirusGuard, the files will already have been copied.

Follow the steps given below:

1. Insert the disk containing GUARD.COM, GUARD.DRV and MESSAGES.DRV in your diskette drive.
   This is usually the Installation Disk 1 of the DOS Anti-Virus Toolkit but it could be on a different diskette. You can check the files on the installation diskettes using the DIR command.

2. Change to that drive by entering `A:` or `B:`, then press ↵.

3. Use the COPY command to copy the files to an appropriate directory on the hard disk. For example, if you are installing to a directory called TOOLKIT on the C: drive, enter the following commands:

```
COPY GUARD.COM C:\TOOLKIT ↵
COPY GUARD.DRV C:\TOOLKIT ↵
COPY MESSAGES.DRV C:\TOOLKIT ↵
```

## Running VirusGuard

To be effective in preventing virus infection, VirusGuard needs to be running on your PC all the time. You can run the GUARD program every time you start up your PC, but it is recommended that you include it in your start-up file so it is run automatically every time you turn on the PC.

Once you have run VirusGuard, it will be resident in memory, taking up about 9 Kb, and will access the virus driver file when necessary. It will remain in memory until you switch off the PC.

### Running VirusGuard manually

1. Change to the drive and directory where the VirusGuard files are stored, for example:

   `CD C:\TOOLKIT` ↵.

2. Type:

   `GUARD` ↵.

### Running VirusGuard automatically

To ensure that VirusGuard is run every time you start up the PC, include the following line in your AUTOEXEC.BAT file.

```
C:\TOOLKIT\GUARD
```

For increased security, include it as near the start of the file as possible so VirusGuard is loaded before other software.

## Using a RAM drive

If you do not have extended or expanded memory on your system, you can run VirusGuard from a RAM drive. This will speed up the virus-scanning process.

A RAM drive is a virtual drive; that is, an area in memory which emulates a very fast, temporary disk drive. Its advantage is that the computer can read information much faster from memory than from a hard disk.

To run VirusGuard from a RAM drive, set up a RAM drive big enough to hold the three files, GUARD.COM, GUARD.DRV and MESSAGES.DRV. If you do not know how to do this, refer to your DOS manual or memory card documentation.

You should then copy the two files to the RAM drive and run them from there. For example, assuming your RAM drive is on the F drive, type:

```
CD \TOOLKIT ↵
COPY GUARD.COM F: ↵
COPY GUARD.DRV F: ↵
COPY MESSAGES.DRV F: ↵
F:\GUARD ↵
```

The main disadvantage with using a RAM drive is that because the drive exists only in memory, information held in it is lost when you turn off the PC. Therefore you have to run the commands above every time you want to run VirusGuard. To save typing this every time you want to load VirusGuard, you could create a batch file containing these commands, and run that instead. Alternatively you could add the commands to your AUTOEXEC.BAT file to load VirusGuard whenever the computer is started up.

## 2.4 Creating a rescue diskette

At the end of the installation process you are reminded to create a rescue diskette. If the formatting of your hard disk is damaged by a virus, you may find that you cannot run DOS properly. A rescue diskette can be used to reboot your PC and repair the damage to the partition sector, boot sector and system set-up information (CMOS data).

To create a rescue diskette, follow the following steps.

1. Create a formatted system diskette.

   If you are using DOS, you can do this by typing:

   `FORMAT A: /S` ↵.

   where `A:` contains the diskette to be formatted.

If you are using Windows, select Format from File Manager and select the Create System Disk option.

Remember that formatting a disk removes all existing data from it.

If you need special drivers to access your hard disk, copy these to the diskette as well, and create an appropriate `CONFIG.SYS` file.

2. Change to the Toolkit subdirectory by typing:

   `CD \TOOLKIT` ↵.

   If you have installed the Toolkit in a different directory, type that name instead of TOOLKIT.

3. Make sure you have the formatted system diskette in the appropriate drive, and that it is not write-protected. Type `RESCUE` and press ↵.

4. A number of files are copied to the rescue diskette. A message appears when the rescue diskette has been created. Make sure you write-protect it, label it and keep it in a safe place.

For details of how to use the rescue diskette, see Chapter 11, "Virus Repair and Removal".

A rescue diskette must *only* be used on the PC on which it was created. If you use it on a different machine, you risk causing serious damage.

## 2.5 README files

As part of the installation, a file called README.DOC is copied to the Toolkit directory. This file contains information that is not included in the manual or the help text, and you should read it carefully.

You can open this file using your normal word processor or editor. Alternatively you can access it from DOS by entering the command:

```
TYPE C:\TOOLKIT\README.DOC
```

If you have installed the Toolkit in a different directory, you should substitute the appropriate path.

## 2.6 Upgrading the Toolkit

The Toolkit is updated monthly to deal with new viruses. S&S recommends that you maintain a subscription to the upgrade service to ensure complete protection from viruses. See "Registration and upgrades" on page xxix.

Upgrades are available on a quarterly or monthly basis, and consist of a complete set of disks. To install the upgrade, follow the steps below for the appropriate version.

### To upgrade the DOS Toolkit

Follow these steps:

1. Boot your PC normally.
2. Insert the diskette labelled Installation Disk 1 of the DOS Anti-Virus Toolkit into the appropriate drive.
3. Change to that drive by typing `A:` and press ↵.
4. At the `A:` prompt, type `INSTALL` and press ↵.
5. Follow the on-screen instructions. When prompted to install VirusGuard:

   ```
   Do you wish to use VirusGuard (Y/N)?
   ```

   reply N, as VirusGuard is already set up from your original installation.

## To upgrade the Windows Toolkit

Follow these steps:

1. Boot your PC normally.
2. Insert the diskette labelled Installation Disk 1 of the Windows Anti-Virus Toolkit into the A drive.
3. Change to that drive by typing `A:` and press ↵.
4. At the `A:` prompt, type `SETUP` and press ↵.
5. Follow the on-screen instructions. When prompted to install VirusGuard and WinGuard, select None, as VirusGuard is already set up from your original installation and select None as the on-access scanners.

# 3. Finding your Way Around

This chapter explains how to start up and use the Toolkit. It explains the differences between the DOS and Windows versions, and explains how to move around the user interface.

## 3.1 Starting the Toolkit

It is strongly recommended that, as an extra precaution, you boot your PC from a clean, write-protected, DOS system diskette before running the Toolkit. This is particularly important if you think you have a virus.

### Starting from DOS

If you have installed the DOS version on the hard disk, after booting the PC, change to the drive and directory containing the Toolkit. For instance, if the files are on the C drive in a subdirectory called TOOLKIT, type:

```
C: ↵
CD: \TOOLKIT ↵
```

Then start the Toolkit:

```
TOOLKIT ↵
```

You can also run the DOS version of the Toolkit from diskette. This offers more security and may be necessary if you have a virus infection on your hard disk. In this case, insert the Installation Disk 1 of the DOS Anti-Virus Toolkit in the appropriate drive and type:

```
A: ↵
TOOLKIT ↵
```

Substitute B: if you are using the B: drive.

There are a number of options you can use when you start up the Toolkit.

If you have an LCD screen, or if the display is difficult to read, there are some display alternatives. For a display in monochrome, enter:

```
TOOLKIT /M ↵
```

For a display in shades of grey, enter:

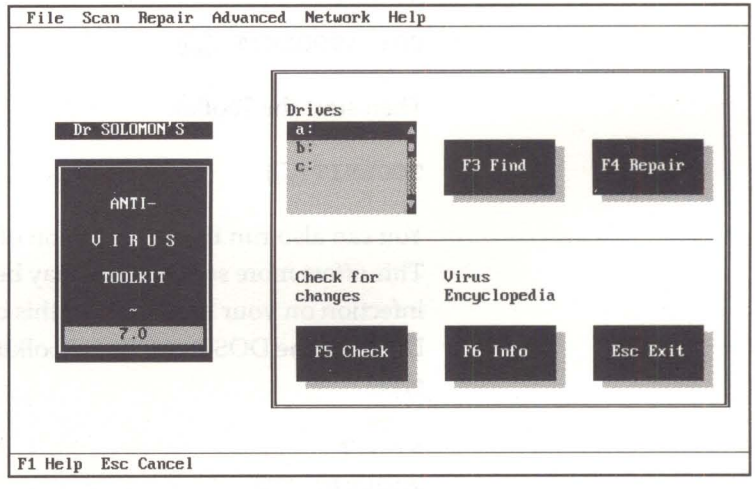
```
TOOLKIT /G ↵
```

To display a block mouse pointer instead of the standard arrow, use:

```
TOOLKIT /NV ↵
```

This can be useful if you are using a laptop or if your display is non-standard.

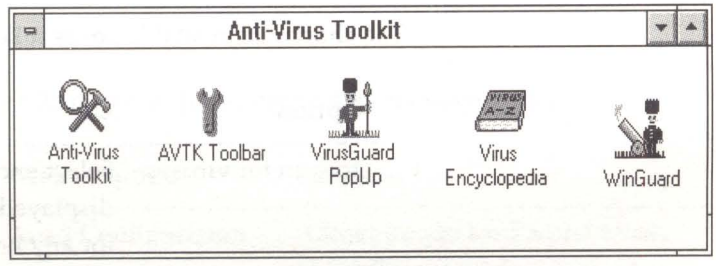
On start up, the DOS main screen is displayed:




See "The main screen" on page 36.

## Starting from Windows

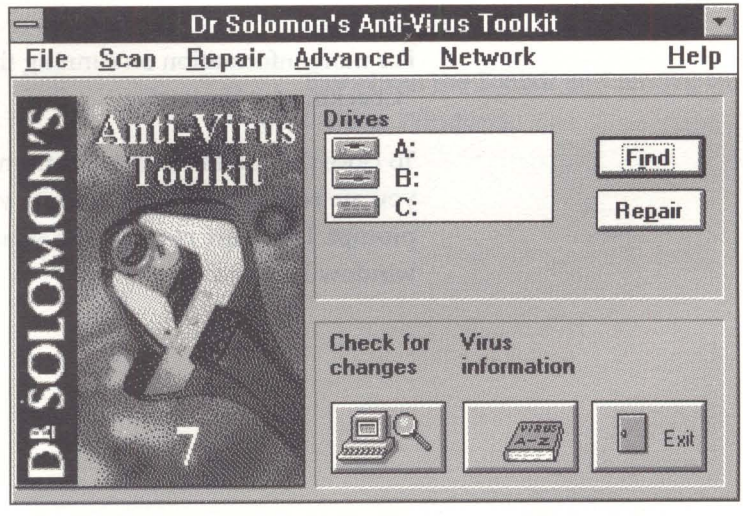
If you have installed the Windows version, the first time you start up Windows after installation, the Anti-Virus Toolkit program group appears:




You can of course move the Toolkit icons to another program group if you wish. See your Windows documentation for full details.

For more information on the Toolkit icons, see "Windows icons" on page xxiii.

To start up the Toolkit, double-click on the Toolkit icon. The following window is displayed:



## 3.2 The main screen

The main screen looks very similar whether you are using DOS or Windows. It provides quick access to the Toolkit's most useful items without having to use the drop-down menus.

The short cuts available are as follows:

| Option | Use |
|---|---|
| To scan for viruses | Select one or more disk drives from the displayed list, then choose Find to scan for any known virus using FindVirus. |
| To repair infected files and sectors | Select a disk drive from the displayed list, then choose Repair to detect viruses and fix the files, boot sectors and partition sectors. |
| To check for changes | The Check for Changes option allows you to perform a check for any changes in executable files, using ViVerify. |
| Displaying virus information | The Virus Information option allows you to browse through the Virus Encyclopedia to find information. |

For more information on running these options, see Chapter 5, "Checking for Viruses".

To close the Toolkit, select Exit from the File menu or press Esc. If you are running the DOS version, you are returned to the DOS prompt. If you are running the Windows version, the Toolkit window is closed.

## 3.3 Options on the menus

Apart from the short cuts on the main screen, you can select the Toolkit features from a number of drop-down menus. These are described below:

### File menu

The File menu includes options for managing files.

| Menu Option | Function |
|---|---|
| Load Configuration | Allows you to load a previously-saved file containing particular Toolkit settings. See Chapter 13, "Toolkit Configuration" for more details. |
| Save Configuration | Allows you to save the current Toolkit settings so that they can be used later. See Chapter 13, "Toolkit Configuration" for more details. |
| Shred | Deletes a file in a way that ensures it cannot be recovered. See Chapter 11, "Virus Repair and Removal" for more details. |
| Exit | Exits from the Toolkit and returns to DOS or Windows. |

## Scan menu

The Scan menu includes a number of options which enable you to set up and run the virus-checking tools.

| Menu Option | Function |
|---|---|
| Find Viruses | Runs FindVirus, which scans for known viruses on any hard disk or diskette. |
| Check for Changes | Runs ViVerify, which can tell if an executable file has been altered. |
| Check Memory | Checks the contents of your PC's memory for common viruses. See Chapter 9, "Advanced Virus Checking". |

## Repair menu

The Repair menu includes the options which allow you to repair infected files and disks.

| Menu Option | Function |
|---|---|
| Repair Drive | Repairs files, boot sectors and partition sectors. |
| Replace Boot Sector | Replaces a corrupted boot sector on a diskette with a clean copy. |

For more details of these options, see Chapter 11, "Virus Repair and Removal".

## Advanced menu

The Advanced menu includes a number of additional options.

| Menu Option | Function |
|---|---|
| Inspect Disk | Allows you to examine a diskette or hard disk at a low level. See Chapter 10, "Additional Tools" for more details. |
| Inspect File | Allows you to examine the contents of a file in ASCII or hexadecimal. See Chapter 10, "Additional Tools" for more details. |
| Inspect Memory | Allows you to examine the first megabyte of PC memory. See Chapter 10, "Additional Tools" for more details. |
| Virus Encyclopedia | Allows you to view the on-line Virus Encyclopedia and to search for particular information. |
| Schedule | Allows you to set FindVirus and ViVerify to run at a particular time. |

Schedule is available only on the Windows version of the Toolkit. It allows you to set up checks for known viruses (FindVirus) or checks for changes (ViVerify) at the times that are most convenient for you. For more information, see "Scheduling FindVirus and ViVerify" on page 67.

An alternative method of scheduling virus checks is available under DOS. See Chapter 14, "Toolkit Utilities" for more information.

# 4. Guarding against Viruses

Although you may run your PC under Windows for most of the time, it is still vulnerable to DOS viruses as well as Windows viruses.

Two memory resident programs are available, both of which scan for viruses whenever files or disks are accessed. If you have installed both programs, as recommended, then one or other of them will be loaded in your computer's memory at all times. These programs detect any signs of a virus infection at the earliest possible opportunity. The two programs are:

- **WinGuard**, a Windows memory-resident scanner (VxD) which takes over from VirusGuard when Windows is run. When both VirusGuard and WinGuard are enabled (as recommended), then control is passed automatically between them as Windows is started up or shut down. Using Windows technology, WinGuard is able to quickly and accurately detect all known viruses, including complex polymorphic ones.

- **VirusGuard**, a DOS memory-resident scanner which scans for viruses whenever an executable file is accessed. It identifies known viruses and prevents access to any file if a virus is found. VirusGuard detects virtually all the viruses in the current driver file. However there are a few particularly complex polymorphic viruses which VirusGuard can detect in memory but cannot prevent from running.

We recommend that you enable both VirusGuard and WinGuard during installation. Using these two scanners, you are fully protected under both DOS and Windows.

## 4.1 Using WinGuard

WinGuard is automatically started when Windows is run and will operate normally without user intervention. The WinGuard status information is displayed momentarily and then minimized as an icon.

If WinGuard is unable to be loaded, Windows will not load either. Instead, a message is displayed. Follow the virus checking instructions in Chapter 5, "Checking for Viruses".

**If a virus is found**

If a virus is detected, access to the file is prevented. In addition, an alarm sounds a dialog is displayed in front of any program you are running

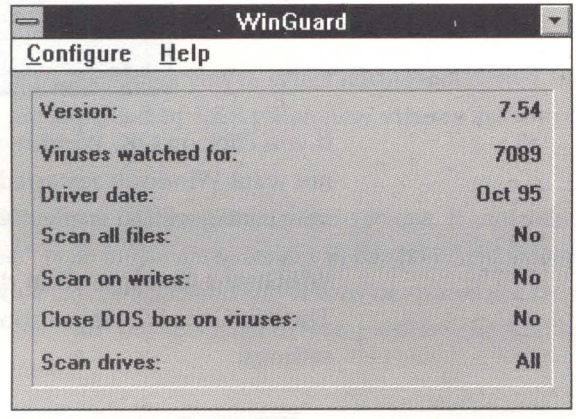
In addition,

- If you are on a network, a separate message can be sent to other users.
- Your application may warn you of a problem. The message and the exact sequence of events will depend on the particular application you are running at the time.

Follow the instructions in Chapter 5, "Checking for Viruses", to run FindVirus on the infected disk and repair the file(s).

## Configuring WinGuard

The WinGuard interface is used to change the configuration. Simply double-click on the icon to open the dialog. The current settings are shown.

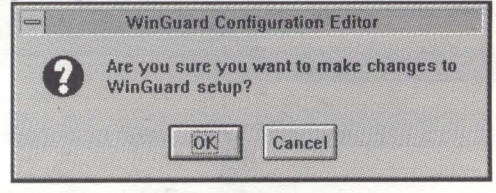



The Configure menu provides two options:

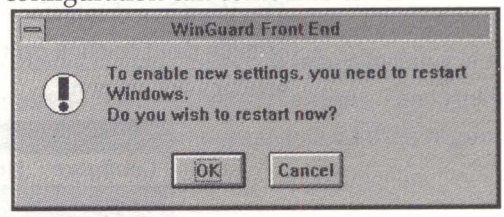
- The WinGuard option allows you to change the settings that govern how WinGuard operates.
- The Front End option defines the messages that will be displayed under different situations when a virus is found.

Full on-line Help is provided from the Help menu and Help is available from within the dialogs.

When you change some settings in either of these dialogs, you see the following prompt:



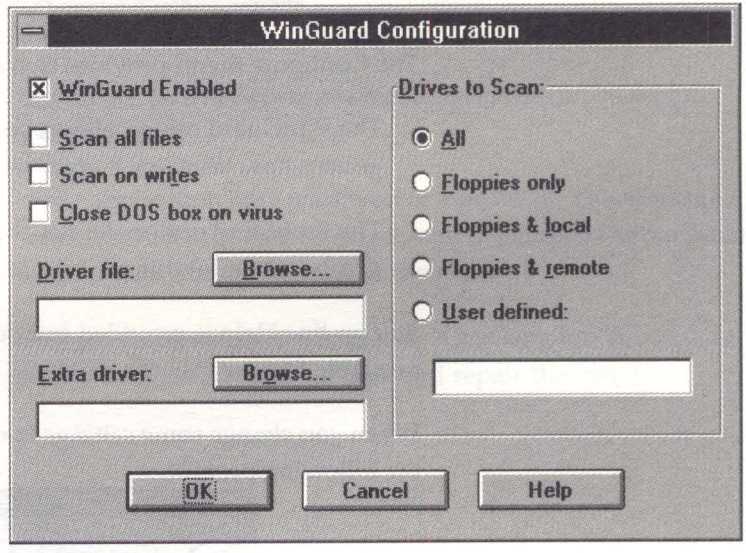
After you click on OK, you are prompted to restart Windows so that the new configuration can come into effect.




If you click on OK, Windows is restarted automatically. If you do not want Windows restarted at this point, click on Cancel. The new configuration is effective only when Windows restarts.

### WinGuard Configuration dialog

The WinGuard Configuration dialog contains a number of settings:




- **WinGuard Enabled**: This option turns WinGuard on and off.
- **Scan all files**: The default setting has this option unselected, so that only files that are most susceptible to virus attack are checked. Click this option so that it is selected if you want *all* files checked.

- **Close DOS box on Viruses**: With this option selected, if a virus is found, the DOS session is closed.

- **Driver file**: Allows you to select other than the FindVirus default driver file. Usually this is only necessary when instructed by S&S Technical Support.

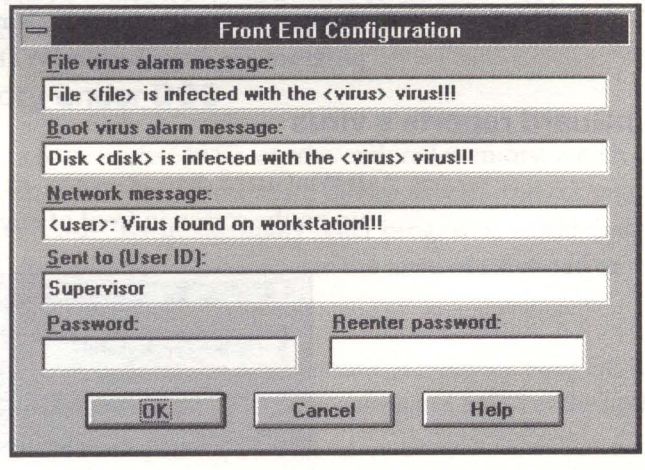
- **Extra Driver**: Allows you to select additional driver files. These are supplied by S&S when new viruses are found in 'the wild'.

- **Drives to scan**: Click on one of the options. If you select "User defined" type in the drive letters in the text field. More than one drive can be specified (no colons or spaces are required). Only files from the specified drive(s) will be checked by WinGuard.

### Front End Configuration dialog

This dialog allows you to change the messages displayed when a virus is detected. The words in angle brackets, < >, will be replaced with the appropriate name(s), when the messages are displayed.

There are four text fields into which you can type a message. You can also enter a configuration password.




- **File virus alarm message**
  The message to display if a virus is found in a file.

- **Boot virus alarm message**
  The message to display if a boot or partition sector virus is found.

- **Network message**
  The message to display if a virus is found by WinGuard on a networked workstation. This message is displayed on one or more workstations, as specified in the Send to (User ID) text field.

- **Send to (User ID)**
  The workstation(s) at which to display the Network Message.

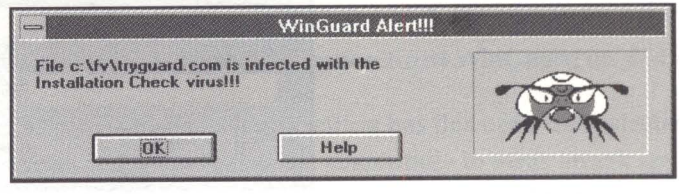
- **Password/Reenter Password**
  By entering a password in these fields, only users who know the password will be able to update the WinGuard configuration. Whenever *either* option is selected from the WinGuard Configuration menu, the user will be prompted for the password. Neither the WinGuard Configuration or the Front End Configuration dialog will be displayed until the password is entered correctly.

## Advanced features of WinGuard

A utility program called WTKUTIL allows you to examine and/or change certain WinGuard settings. The options offered by this program are described in "WTKUTIL command" on page 191.

## If WinGuard reports a virus

If WinGuard detects a virus, an alarm sounds and a warning pops up on the screen in front of any program you are running.




The pop-up tells you what has caused the WinGuard alarm and which file or disk has caused the problem.

You will not be able to copy or run the infected file.

If the alarm is sounded and displayed, follow these steps:

1. Read the message in the pop-up and then press the Ctrl key, or select OK.
2. Exit in the normal way from whatever you were doing and save any files you were working on.
3. Shut down Windows.
4. Power off and boot the PC from a clean, write-protected, DOS system diskette.
5. Run DOS FindVirus from the original DOS Toolkit installation diskette to scan the appropriate disk.

Chapter 6 gives details of how to remove a virus and repair files.

## 4.2 Using VirusGuard

If you specified, during installation, that VirusGuard should run automatically, then it runs each time the computer is started up. It is disabled as Windows is started and re-enabled if you exit to DOS, and operates without user intervention.

### How VirusGuard uses memory under DOS

Most PCs have up to 640 Kb of conventional memory, which is used to run DOS and the standard device drivers and commands. However, VirusGuard, like many other programs, works faster if your PC has additional resources in the form of extended or expanded memory.

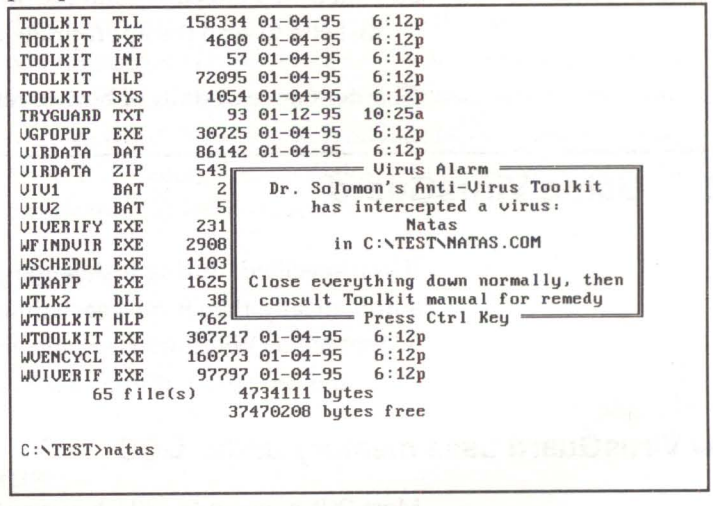
If you are unsure of the type or amount of memory your PC has, you can find out by typing the DOS command MEM at the system prompt.

If you have expanded or extended memory, VirusGuard automatically uses the most appropriate memory option when it runs. It checks for extended memory first, and if this is not present, or if there is not enough contiguous extended memory available, it looks for expanded memory.

If necessary, VirusGuard can make use of a RAM drive, or even access the virus driver file from the hard disk (provided that the GUARD.COM and DRV files are copied there and run from there).

## If VirusGuard reports a virus

If VirusGuard detects a virus, an alarm sounds and a warning pops up on the screen in front of any program you are running.




The pop-up tells you what has caused the VirusGuard alarm and which file or disk has caused the problem.

You will not be able to copy or run the infected file.

If the alarm is sounded and displayed, follow these steps:

1. Read the message in the pop-up and then press the Ctrl key, or select OK.

2. Exit in the normal way from whatever you were doing and save any files you were working on.

3. Return to the system prompt.

4. Power off and boot the PC from a clean, write-protected, DOS system diskette.

5. Run DOS FindVirus from the original DOS Toolkit installation diskette to scan the appropriate disk.

Chapter 6 gives details of how to remove a virus and repair files.

# 5. Checking for viruses

This chapter provides a step-by-step explanation of running FindVirus and ViVerify from the user interface. For details of how to run the programs from the command line or in batch files, see Chapter 7, "Advanced Virus Detection" and Chapter 9, "Advanced Virus Checking".

It is strongly recommended that, as an extra precaution, you boot your PC from a clean, write-protected, DOS system diskette before running the Toolkit. This is particularly important if you think you have a virus.

## 5.1 Finding viruses - FindVirus

FindVirus scans for all the boot sector, partition sector and file viruses listed in the virus driver file. You can use FindVirus to ensure that any hard disk or diskette is free from all known viruses.

An option also allows you to run a heuristic scanner. This technique looks inside files for suspect code combinations that may be a result of new viruses not yet included in the virus driver file.

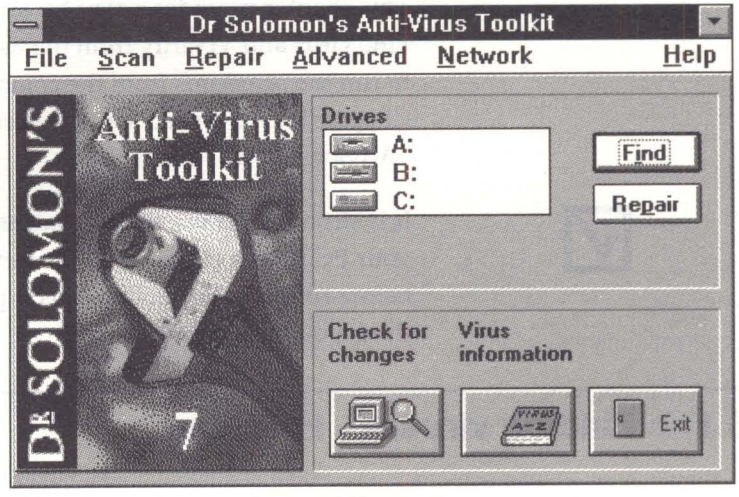
### When to use FindVirus

You should use FindVirus to scan all incoming diskettes and files to ensure they are free from viruses.

You can also use FindVirus to help clean up after a virus outbreak. It will tell you which files are infected, and with what virus. It can also be used to repair the virus infections.

## Running FindVirus from the main screen

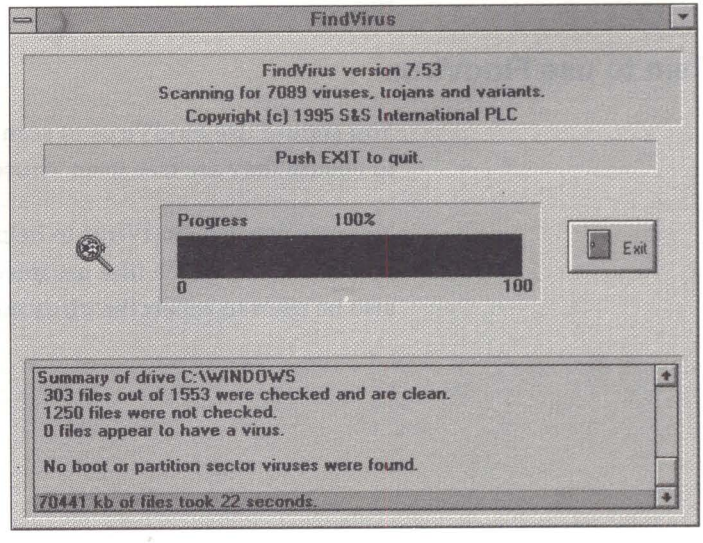
You can run FindVirus from the Toolkit main screen:




Follow these steps:

1. In the Drives box, select the drive(s) you want to check.

2. Select Find. The selected drives are scanned for viruses. When each scan is complete, a report of the following format is displayed:


FindVirus
FindVirus version 7.53
Scanning for 7089 viruses, trojans and variants.
Copyright (c) 1995 S&S International PLC
Push EXIT to quit.
Progress 100%
0
100
Exit
Summary of drive C:\WINDOWS
303 files out of 1553 were checked and are clean.
1250 files were not checked.
0 files appear to have a virus.
No boot or partition sector viruses were found.
70441 kb of files took 22 seconds.

3. If you have selected a diskette drive, when the scan is complete, you will be asked if you want to scan another diskette. If so, insert the next diskette before choosing Yes.

4. If your disk is free from viruses, the message *All clear* is displayed.

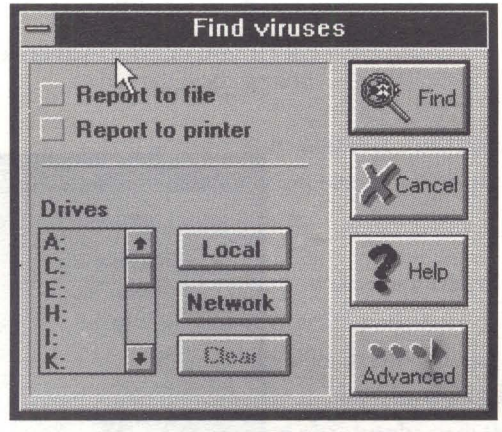
If a virus is found, do not panic! See Chapter 6, "If you Find a Virus", for information about what to do.

Running FindVirus from the main screen uses the default settings. If you want to change any of these, you should run FindVirus from the Scan drop-down menu as described in the next section.

## Running FindVirus from the user interface

To run FindVirus from the user interface:

1. Select Find Viruses from the Scan menu. The following dialog box is displayed:




2. The settings and options are as follows:

Report to — By default, a report of the scan is displayed on the screen. In addition, you can choose to direct the report to a file, to a printer or to both.

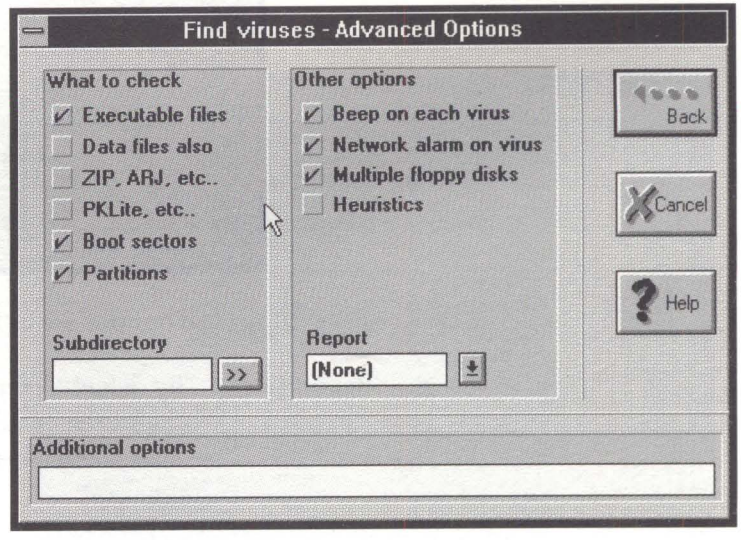
If you choose Report to file, the report will be saved in a file called FINDVIRU.REP in the TOOLKIT directory. You can change this filename using a setting on the Advanced dialog box.

If you choose Report to printer, the report will be sent to your default system printer. Make sure it is connected, loaded with paper and on-line.

Drives — Select the drives you want to scan. Choose Local to scan all the hard drives on your PC. Select Network to scan all network drives. Select Clear to clear any selections you have made.

3. These settings are suitable in most cases. You can start the scanning process by selecting Find or pressing ↵. Additional options are available by selecting the Advanced dialog box.

4. If you choose Advanced, the following dialog box is displayed:



5. The settings and options are as follows:

What to check — By default, FindVirus scans filesmost susceptible to virus infection, boot sectors and partition sectors. You can change these settings if you wish.

Select Data files to scan all non-executable files. Normally, you need only select this option if you are cleaning up after a virus infection.

Select ZIP, ARJ to scan files which have been archived using ARC, PKZip, LZH or ARJ. .

Select PKLite if you want FindVirus to scan files compressed using PKLite, LZExe, ICE, Diet or CryptCom.

You should only deselect Boot sectors if this causes a particular problem, for example if you are scanning a network drive that doesn't have a boot sector.

You should only deselect Partitions to suppress partition sector scanning when this causes a problem.

Subdirectory — If you only want to scan a particular subdirectory, enter its path here. FindVirus then only scans files in the named directory and those below it. You should only use this option if you are absolutely sure that the virus is in a particular location, for example, if VirusGuard has reported a virus, and you haven't run anything since. It is always much safer to scan the entire drive.

Other options — Select Beep on each virus if you need this extra warning when a virus is found.

Choose Network alarm on virus to send a message to the network supervisor. This option is only visible if your PC is connected to a network.

Choose Multiple floppy disks if you want to scan more than one diskette in the same drive. You are prompted to insert the next diskette when each one has been scanned.

Choose Heuristics when it is necessary to scan for unknown viruses, and after any known ones have been eliminated.

Report — If you want to send the virus report to a file, you can specify a filename here. The default filename is FINDVIRU.REP.

Additional options — This shows the DOS command line for the options you have chosen. You can modify this directly if you wish. A full description of the various switches is given in Chapter 7, "Advanced Virus Detection".

6. When you have set any additional advanced options, select Back to return to the main FindVirus dialog box. Then select Scan to start the scan.

7. If your disk is free from viruses, the message *All clear* is displayed.

If a virus is found, do not panic. See Chapter 6, "If you Find a Virus", for information about what to do.

You can save the changed FindVirus settings for future use. Select Save Configuration from the File menu. For more information, see Chapter 13, "Toolkit Configuration".

## 5.2 Checking for changes - ViVerify

ViVerify enables you to detect changes in executable files which may be the result of a virus infection. ViVerify works by calculating a unique fingerprint, or checksum, for each file it is protecting. This fingerprint can then be recalculated at any time as a safety check to see if any changes have been made. ViVerify also detects changes in boot and partition sectors.

With this type of tool, you need a balance between speed and security. If the fingerprint calculations are too complex, ViVerify will take a long time to run. On the other hand, if the calculation is too simple, it is possible for a virus to evade detection. This is known as *spoofing*. ViVerify's default settings are a good balance between security and performance. However, you can change the settings if necessary to choose the level of security you want.

ViVerify's default fingerprinting method makes use of a keyword. You have to enter a keyword when the fingerprints are first calculated, and then repeat it every time a check is performed. This increases security by preventing a virus from spoofing the fingerprint.

### When to use ViVerify

You can use ViVerify to check executable files on a regular basis.

You can also use ViVerify when cleaning up after a virus infection, as it gives early warning of possible re-infection which can be dealt with before it spreads to other PCs.

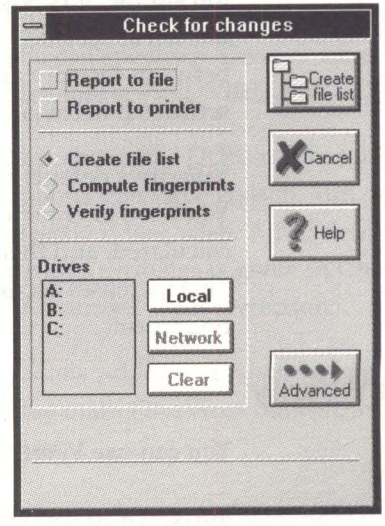
## Running ViVerify

You can run ViVerify in two ways:

- From the Toolkit main screen by selecting the Check for Changes box.
- By selecting Check for Changes from the Scan menu.

The dialog boxes and options are exactly the same for both methods.

1. When you select **Check for Changes**, the following dialog box is displayed:




2. The settings and options are as follows:

Report to — By default, a report of the process is displayed on the screen. In addition, you can direct the report to a file, to a printer, or both. If you select Report to file, the report is saved in a file called VIVERIFY.REP in the TOOLKIT directory. (You can change this filename using an option on the Advanced dialog box.)

If you choose Report to printer, the report is sent to your default system printer. Make sure it is connected, loaded with paper and on-line.

Drives — Select the drives you want to check. Choose Local to scan all the hard drives on your PC. Select Network to check all network drives. Select Clear to clear any selections you have made.

Keyword — This box only appears when you have selected Compute fingerprints or Verify fingerprints. This is used to encrypt the fingerprints, providing an additional level of protection.

3. These options are suitable for most cases. Additional options can be specified in the Advanced dialog box.

There are three stages in running ViVerify:

- Create a list of the files that you want to check using the Create file list option.
- Calculate the unique fingerprints for each file, using the Compute fingerprints option.
- Regularly check the set of files for changes, using the Verify fingerprints option.

These three stages are described below.

## Creating a file list

To create a list of files to check:

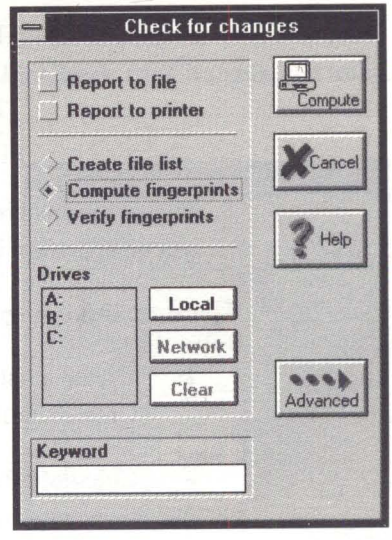
1. Select Create file list.
2. Select the drives to be checked. For example, select Local to make a list for all local hard disk drives.
3. Press the Create file list button, or press ↵.

4. ViVerify checks the disk for executable files. When the file list has been created, a message is displayed. Press any key (or click the mouse) to return to the main screen.

## Computing the fingerprints

To calculate fingerprints for the selected files:

1. Select Compute fingerprints. The dialog box changes slightly:




2. Select the drives to be checked. For example, select Local to make a list for all local hard disk drives.

3. Select the Keyword box. Type in a word of at least eight alphanumeric characters. This keyword is then used as part of the encryption process, which helps prevent a virus from simulating the correct fingerprints.

Note: The keyword is not a password. It is quite safe to write it down and keep it next to the PC - a virus cannot read it!

4. Press the Compute button, or press ↵.

5. When the fingerprints have been calculated, a message is displayed. Press any key (or click the mouse button) to return to the main screen.

## Checking the files

Once you have selected the files and computed the fingerprints, you should check them on a regular basis. To check the fingerprints for the selected files:

1. Select Verify fingerprints.
2. Select the drives to be checked. For example, select Local to check the fingerprints for all local hard disk drives.
3. Select the Keyword box. Enter the keyword used previously.
4. Press the Verify button, or press ↵.
5. When the fingerprints have been verified, a message is displayed. Press any key (or click the mouse button) to return to the main screen.

## If a file has changed

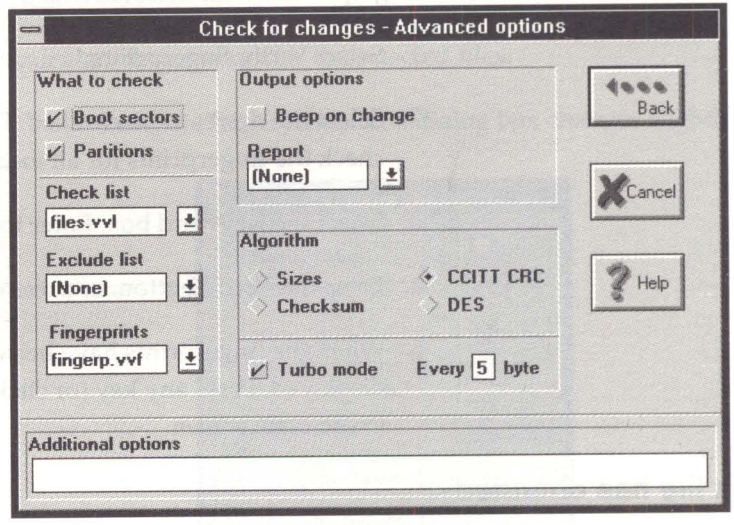
If ViVerify indicates that a fingerprinted file has been changed, this does not necessarily mean that you have a virus infection. Other possibilities are:

- The changed files could be data files. Data files will always change when they are modified, and occasionally they have names that make them look like executable files.
- Some EXE and COM files are altered by installation routines.
- If ViVerify reports that all programs have been changed, don't panic. It probably means that you have entered the keyword incorrectly. Check this and run it again before wasting time on an unnecessary clean-up operation.

However, if a number of files have changed unexpectedly, it is possible that you have a virus. See Chapter 6, "If You Find a Virus" for information about what to do next.

## Advanced menu options

If you select the **Advanced** box from the **Check for Changes** screen, a further screen is displayed:




The settings and options are as follows:

What to check — ViVerify always checks executable files. By default, boot and partition sectors are also checked. You should only deselect boot sectors if this causes a particular problem, for example on a network drive which doesn't have a boot sector. You should only deselect Partitions to suppress partition sector checking when this causes a problem.

Check list — This identifies the file that contains the list of files to be checked. The default file name is FILES.VVL. The latest version of the file always overwrites the previous one. If you want to check more than one drive in separate runs of the program, you may wish to create a separate list for each drive, for example, C_FILES.VVL. These files are created in the default Toolkit directory unless you specify otherwise.

Exclude list

A number of files may be excluded from the checking process. This parameter identifies the file that holds this list. The default filename is EXCLUDE.VVX. You can add files to this list, or change the filename if you wish. For more details, see Chapter 9, "Advanced Virus Checking".

Fingerprints

The fingerprints created for the files checked are stored in a file called FINGERP.VVF. You can specify a different filename if required.

Output

If Beep on change is selected, the PC beeps every time ViVerify finds a changed file.

The Report option is valid only if you have opted to send the checking report to a file. If you want to check more than one drive in separate runs, the latest report will overwrite the previous one. Therefore you may want to create a separate report for each drive, for instance C_VER.REP, D_VER.REP, etc. These files are created in the default Toolkit directory unless you specify otherwise.

Algorithm

This box indicates the method used for calculating the fingerprints. The default calculation method is the CCITT Cyclic Redundancy Check, which is suitable for most users.

The Size algorithm calculates fingerprints based on the file size. This is a very fast calculation, but a few viruses do not change the size of files they infect, and therefore can evade it.

The Checksum algorithm calculates the fingerprints as a sum of the bytes checked in the files. The keyword is also incorporated.

The DES option calculates the fingerprints using the standard Data Encryption Standard algorithm, incorporating the keyword. This is very secure but requires lengthy calculations. Only use this option if your company policy requires this level of security.

More details on encryption methods are given in Chapter 9, "Advanced Virus Checking".

**Turbo mode** By default, ViVerify checks just the first and last 4 Kb of each file by default. This speeds up the calculation. It is very unlikely that a virus could infect your system without changing at least one byte in these areas. You can deselect turbo mode if required.

**Every n byte** Checking every byte in a file would be very time-consuming. By default, ViVerify checks every fifth byte. You can speed up the checking by increasing this number, or increase security by choosing a lower number.

**Additional options** This shows the DOS command line for the options you have chosen. You can modify this directly if you wish. A full description of the various parameters and switches is given in Chapter 8 "Advanced Virus Checking".

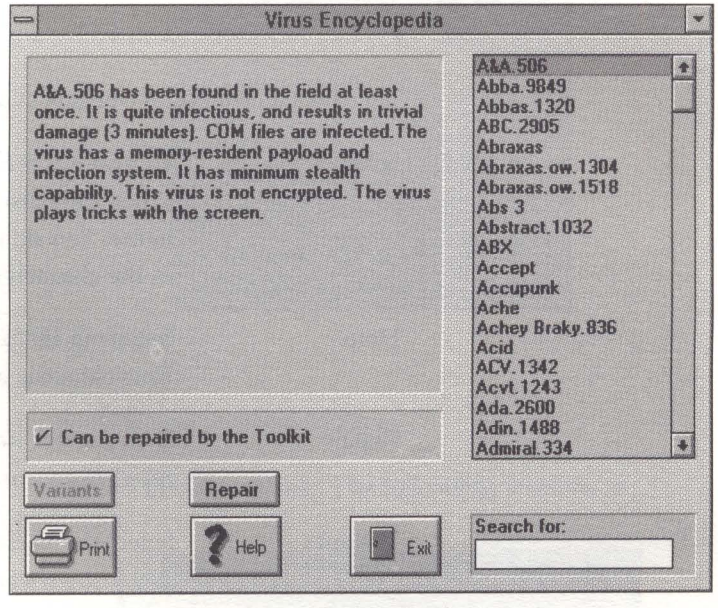
You can save the changed ViVerify settings for future use. Select Save Configuration from the File menu. For more information, see Chapter 13, "Toolkit Configuration".

## 5.3 The Virus Encyclopedia

The on-line Virus Encyclopedia contains details of all the viruses recognized by the Toolkit. You can view the Encyclopedia in two ways:

- From the Toolkit main screen by selecting the Virus Information button.
- By selecting Virus Encyclopedia from the Advanced drop-down menu.

The following screen is displayed: :




You can display information about a virus by selecting it from the list. You can scan through the list using the scrollbars.

For each virus, the Encyclopedia gives the following information:

- How common it is.
- How infectious it is.
- How much damage it does.
- What is infected: files, boot sectors or partition sectors.
- Whether or not it has memory-resident capabilities.
- If it uses stealth.
- If it is polymorphic.
- Any aliases it is known by, and whether there are any variants.

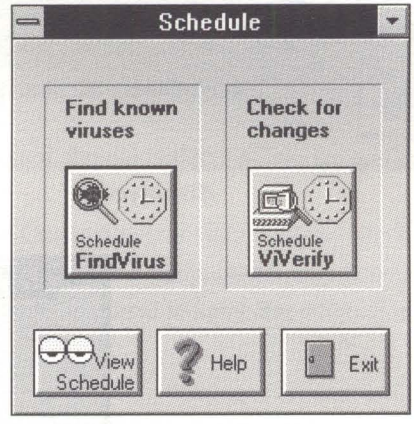
There are a number of options available from this screen:

| | |
|---|---|
| Search | To find out information about a particular virus, move to the Search box and type its name. You do not need to press ↵, just type in the characters. |
| Help | Selecting Help displays information about the Encyclopedia and how to use it. |
| Repair | If you select Repair, help information about repairing viruses is displayed. |
| Variants | Select the Variants box to display the names of any known variants. |
| Print | Prints the displayed information about the selected virus. |

## 5.4 Scheduling FindVirus and ViVerify

The Schedule feature is only available in the Windows version of the Toolkit. It allows you to run FindVirus and ViVerify at specified times. This allows you to scan for viruses and check for changes at the times that are most convenient for you.

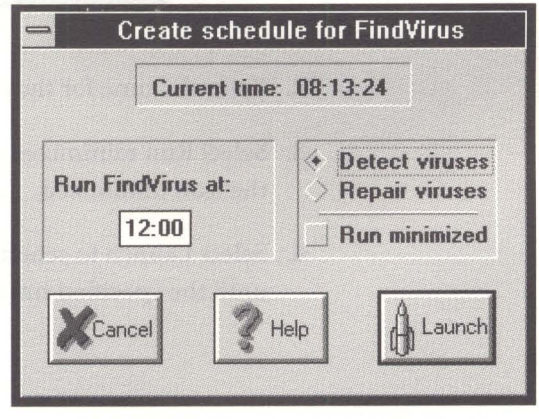
The Schedule feature is selected from the Advanced menu. When it is selected, the following window is displayed:




### To schedule FindVirus

To run FindVirus at a specified time:

1. Select Find known viruses. The following window is displayed:

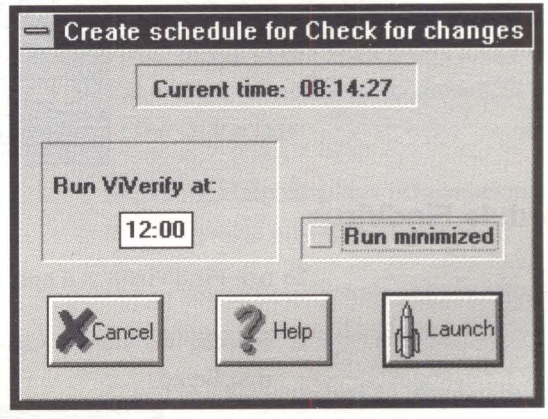


2. Enter the time for the scan to be run, in 24-hour clock format.
3. Select either Detect viruses if you want to find and report on any viruses or Repair viruses if you want FindVirus to automatically repair any infected files found.
4. If you select Run minimized, the program is run with the icon minimized.
5. Select Launch to schedule the virus check. The icon is minimized until the specified time.

## To schedule ViVerify

To run ViVerify at a specified time:

1. Select **Check for Changes**. The following window is displayed:

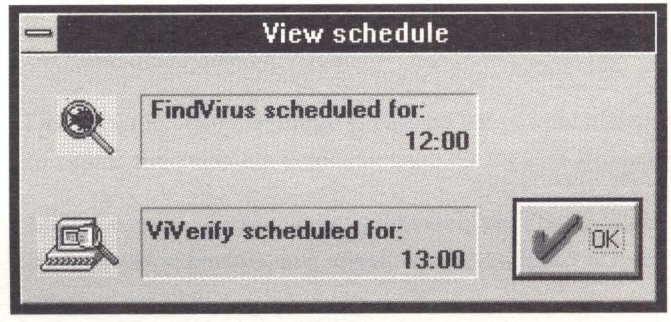



2. Enter the time for the check to be run, in 24-hour clock format.
3. Select Run minimized if you want the program to be run with the icon minimized.
4. Select Launch to schedule the check. The icon is minimized until the specified time.

## Checking the schedules

Once you have set up a schedule, the appropriate icon is minimized on the screen.

You can display the current schedule by selecting View Schedule:




If you click on the Control-menu button at the top left-hand corner of the Schedule box, a drop-down menu appears. Select Save Schedule from this menu to save the current settings.

# 6. If you Find a Virus

This chapter tells you how viruses are reported from the various Toolkit programs, and explains the steps you need to follow to remove the virus and carry out any necessary repairs to files, boot sectors and partition sectors.

If you have discovered a virus:

- Don't panic. More damage is caused by people attempting to repair the problem wrongly than by viruses themselves.
- Make sure you know what action to take. The Toolkit includes straightforward repair methods. Read through this chapter carefully.
- If you are in any doubt, leave the computer turned off.
- If your company has procedures for dealing with viruses, you should follow them.

## 6.1 If VirusGuard or WinGuard report a virus

If VirusGuard or WinGuard detects a virus, an alarm sounds and a warning pops up on the screen in front of any program you are running.

The pop-up tells you what has caused the alarm and which file or disk has caused the problem. If you are running DOS, the warning is as follows:

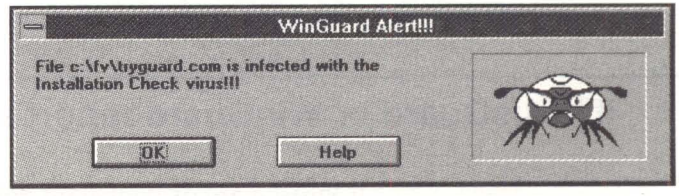
```
TOOLKIT  TLL    158334 01-04-95   6:12p
TOOLKIT  EXE      4680 01-04-95   6:12p
TOOLKIT  INI        57 01-04-95   6:12p
TOOLKIT  HLP     72095 01-04-95   6:12p
TOOLKIT  SYS      1054 01-04-95   6:12p
TRYGUARD TXT        93 01-12-95  10:25a
VGPOPUP  EXE     30725 01-04-95   6:12p
VIRDATA  DAT     86142 01-04-95   6:12p
VIRDATA  ZIP       543
VIV1     BAT         2
VIV2     BAT         5
VIVERIFY EXE       231
WFINDVIR EXE      2908
WSCHEDUL EXE      1103
WTKAPP   EXE      1625
WTLK2    DLL        38
WTOOLKIT HLP       762
WTOOLKIT EXE    307717 01-04-95   6:12p
WVENCYCL EXE    160773 01-04-95   6:12p
WVIVERIF EXE     97797 01-04-95   6:12p
       65 file(s)    4734111 bytes
                    37470208 bytes free

C:\TEST>natas
```

```
Virus Alarm
Dr. Solomon's Anti-Virus Toolkit
has intercepted a virus:
Natas
in C:\TEST\NATAS.COM

Close everything down normally, then
consult Toolkit manual for remedy
Press Ctrl Key
```

If you are running Windows, then WinGuard will display an alarm screen, for example:




You will not be able to copy or run the infected file

## What to do if VirusGuard or WinGuard sounds the alarm

Follow these steps:

1. Read the message in the pop-up and then press the Ctrl key, or select OK.

2. Exit in the normal way from whatever you were doing and save any files you were working on.

3. Return to the system prompt.

4. Power off and boot the PC from a clean, write-protected, DOS system diskette.

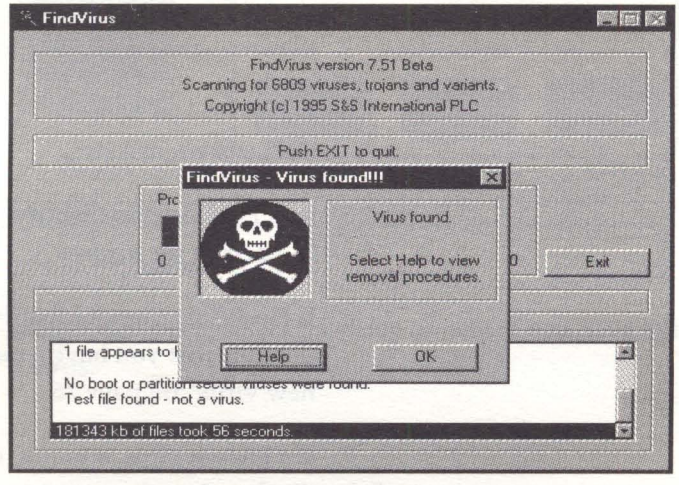
5. Run FindVirus to scan the appropriate disk.

Don't worry if FindVirus calls the virus by a different name from that reported by VirusGuard. FindVirus is more precise about names and the name it gives is the right one.

For details of how to repair the virus infection, see "Single button repair" on page 75.

## 6.2 If FindVirus reports a virus

Whenever you run FindVirus, it displays a screen of information. If a virus is found, it sounds an alarm and displays details of the virus in the report, in the following format:




### What to do if FindVirus discovers a virus

Follow these steps:

1. Read the message and make a note of the virus found.

2. Exit in the normal way from whatever you were doing and save any files you were working on.

3. Return to the system prompt.
4. Power off and boot the PC from a clean, write-protected, DOS system diskette.

For details of how to repair the virus infection, see "Single button repair" on page 75.

## 6.3 If ViVerify reports a changed file

If ViVerify reports that a number of files have changed unexpectedly, it is possible that you have a virus.

### What to do if changed files are reported

1. Note the names of the changed files reported by ViVerify.
2. Exit in the normal way from whatever you were doing and save any files you were working on.
3. Return to the system prompt.
4. Power off and boot the PC from a clean, write-protected, DOS system diskette.
5. Run FindVirus to identify the virus (see Chapter 5, "Checking for Viruses").
6. If FindVirus cannot identify a virus in the changed files, it is possible that you have a new virus. See "If you discover a new virus" on page 76.
7. If a known virus is found, make a note of the details displayed on the report screen.

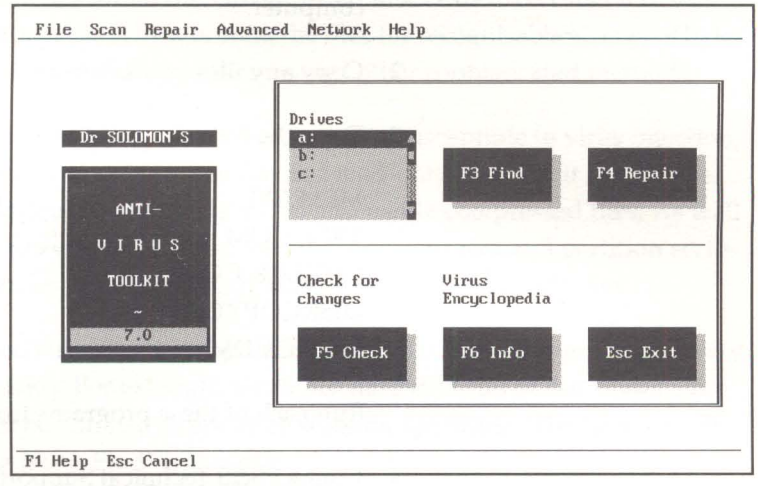
For details of how to repair virus infections, see "Single button repair" on page 75.

## 6.4 Single button repair

The Toolkit includes a straightforward facility for repairing infected files, boot sectors and partition sectors.

You should boot your PC from a clean, write-protected DOS system diskette before repairing files. For maximum security, it is recommended that you run the Toolkit from DOS.

The single-button repair can be run from the main screen:




Carry out the following steps.

1. In the Drives box, select the drive on which you have found a virus.

2. Select Repair.

The repair program operates as follows:

1. Any infected files are repaired, if possible. If a file cannot be repaired, it is renamed. The first character of each file extension is changed to a V. For example COM is changed to VOM and EXE to VXE.

2. If the boot sector of a diskette is infected, it is replaced with a clean boot sector.

3. If the partition sector of a hard disk is infected, it is replaced with a clean partition sector.

When the repair is complete, it is recommended that you run FindVirus again to check that the disk is free from viruses.

## 6.5 If you discover a new virus

If you suspect a new virus:

1. Boot normally and format a diskette in the infected computer.
2. Copy any files you know are infected to the diskette.
3. Copy the following additional files to the diskette:

   MEM.EXE
   TREE.COM
   CHKDSK.COM
   DISKCOPY.COM
   MODE.COM

   Run each of these programs from the diskette.
4. Contact S&S Technical Support directly, or your authorized distributor.
5. Do not run anything on the infected PC. If the PC is attached to a network, disconnect it to prevent other users from accessing any files.

S&S can tell you whether the problem is a virus or not, and what you need to do. See "If you need help" on page xxx.

# 7. Advanced Virus Detection

This chapter includes technical information on using FindVirus, including running the program from the command line or from within batch files.

## 7.1 How FindVirus works

FindVirus, with the default scanner, scans your hard disks and diskettes for all the viruses listed in a virus driver file. It detects viruses them by scanning the files for recognisable strings of bytes from within the virus code, and other sophisticated methods.

By default, FindVirus scans all files susceptible to virus infection, including system, hidden and read-only files, but it can also be configured to scan data files and inside compressed files. As well as file viruses, it looks for boot sector viruses and partition sector viruses. FindVirus also finds common trojans and jokes.

FindVirus has been optimized for virus scanning, so it works very quickly. For example, an 80 Mb hard disk full of executable files can be scanned in about 20 seconds. Obviously, the faster the PC, the faster FindVirus works.

FindVirus can be run from the Scan drop-down menu, or directly from the main screen by selecting Find. Details of using it in this way are given in Chapter 5, "Checking for Viruses". Alternatively, you can run it from the DOS command line or within a batch file.

If you think you may have a virus, you are recommended to boot your PC from a clean, write-protected, DOS system diskette before running the Toolkit. The most secure way to run FindVirus is from a write-protected diskette.

Because FindVirus scans for the specific viruses within the virus driver file, it is vital that this file is kept up-to-date. If your version is out-of-date, a message is displayed to that effect when you run FindVirus. See "Registration and upgrades" on page xxix.

## Heuristic Analysis

Heuristic analysis is a technique for finding new viruses. It looks inside files for the code combinations necessary for a virus to operate.

For most installations, FindVirus used with the default setting provides more than ample protection against viruses. Where more security is required, for example, on a machine where many floppy disks are used or a large number of new executable file are processed, it would be advisable to enable the Advanced Heuristic Analyser. This will increase scanning times by approximately 50%.

To invoke Heuristic Analysis from the User Interface, Heuristic scanner must be selected from the Advanced Options dialog.

At the command line, for a diskette in the A drive, use the following switch for heuristic analysis:

```
FINDVIRU A:  /ANALYZE
```

When a possible virus has been found by the Heuristic Analyser, you see the following message on the screen:

```
<filename.ext> could be a new virus!!!
Send a specimen to S&S
```

Contact S&S Technical Support using the information "If you need help" on page xxx.

## Executable files

File viruses only infect executable program files; these may include some data files containing executable macros. By default, FindVirus scans for files with the following extensions:

| | |
|---|---|
| APP | DOT |
| BAT | EXE |
| BIN | OV? |
| CMD | QLB |
| COM | SYS |
| DEV | XTP |
| DLL | 001 |
| DOC | 002 |

If you have executable files with other extensions, you should set FindVirus up to scan for all files. In its default mode, FindVirus scans every executable file in every subdirectory on a disk.

## Compressed and archived files

FindVirus can scan for viruses in files that have been compressed using many common archiving programs. It achieves this by decompressing as much of the files to memory as necessary and then scanning them for viruses. Because the PC's available memory is used to decompress files, it does not need any hard disk space or access to diskettes.

FindVirus can scan files compressed using the following tools:

| | |
|---|---|
| ARJ | LZExe |
| CryptCom | ARC |
| Diet | PKLite |
| ICE | PKZip |
| LZH | |

By default, scanning of compressed files is turned off.

FindVirus can also scan inside "unextractable" PKLited files.

Self-extracting archived files, such as those created with the PKWare utility ZIP2EXE can also be scanned.

If you have multiple-level archived files, such as ARJ files within ZIP files, FindVirus recursively decompresses all levels and scans them completely for viruses if enough memory is available.

When scanning compressed executable files, FindVirus reports that it has scanned the self-extractor code and then that it has scanned the contents of the compressed file. This does not mean that the same file is scanned twice.

If you have ZIP or ARJ files which have been encrypted with passwords, FindVirus is unable to scan them for viruses. In these instances it displays a message at the end of the scan warning that password-encrypted files were found and have not been scanned. For complete security you should unpack these files manually and decrypt them before scanning them.

Scanning compressed and archived files slows down FindVirus and is really only necessary for sheep-dip PCs.

The ability to scan within compressed and archived files is only available on PCs with 386 processors or above.

## Repairing files

FindVirus can also be run with the Repair option, to remove viruses and repair executable files. It attempts to remove any viruses and restore the files.

For more information, see Chapter 11, "Virus Repair and Removal".

## 7.2 Running FindVirus from the user interface

You can run FindVirus from the user interface in the following ways:

- From the main screen, by choosing the drives to be scanned and selecting Find.
- By selecting Find Viruses from the Scan menu.

These options are explained in detail in Chapter 5, "Checking for Viruses".

## 7.3 Running FindVirus from the command line

You can run FindVirus from the command line or within a batch file.

The command syntax is:

```
FINDVIRU [switches]
```

The action of the switches is discussed in the following sections. You cannot use any switch more than once on the command line. For example, only the first `/LOCAL` has any effect. The switches must be separated by spaces and they can be typed in upper or lower case. You can display the most common switches by running FINDVIRU with the `/?` or `/HELP` switches.

### Scanning specific drives

The most common way of defining the drive to be scanned is to specify the drive on the command line. For example:

```
FINDVIRU C:
```

to scan the C: drive.

Alternatively, you can use one of the following switches:

```
/D=
/ALLDRIVES
/LOCAL
```

If you do not specify a drive, FindVirus prompts for the drive to be scanned.

The `/D=` switch allows you to specify one or more particular drives.

| | |
|---|---|
| `/D=`*`drive`* | Scans the specified drive(s). |

For each drive you want to scan, enter the identifying letters, without spaces between them. You do not need to enter the colon. For example:

```
FINDVIRU /D=CD
```

scans the C: and D: drives.

| | |
|---|---|
| `/ALLDRIVES` | Scans all fixed disk drives, including network drives. |
| `/LOCAL` | Scans the current local hard disk drives. |

If you specify a diskette drive, FindVirus will automatically scan a number of diskettes in the same drive. For example:

```
FINDVIRU /D=A
```

Once each diskette has been scanned, you will prompted to remove it and insert the next. You can change this default with the following switches:

| | |
|---|---|
| `/ONEONLY` | Scans one diskette only, and does not prompt for further diskettes. |
| `/PAUSE` | Pauses after loading a diskette. |

For example:

```
FINDVIRU /D=A /ONEONLY
```

scans just one diskette in drive A:, and does not prompt for further diskettes.

## Scanning files and subdirectories

By default, FindVirus scans all executable files on the specified drive. You can specify particular files to be scanned with a number of switches.

To scan data files as well as executables, use the `/DOALLFILES` switch. For example:

```
FINDVIRU /LOCAL /DOALLFILES
```

scans all files (executable and data) on the local hard drive.

Viruses do not infect data files, so this option is unnecessary for most situations. Normally, you need only use it when you are cleaning up after a virus infection.

If you want to scan a particular set of files, you can use the `/CHECKLIST` option:

`/CHECKLIST=`*`file`* Scans only the files listed in the specified file.

You can create a file containing the names of the files you want FindVirus to scan using a text editor or word processor. This must be an ASCII file containing only the filenames, including extensions, one filename on each line. Do not include drive or path specifiers.

You can also use this option to scan suspect files included in a list produced by ViVerify with the `/BADLIST` option. See "Producing a list of suspect files" on page 123.

For example:

```
FINDVIRU /CHECKLIST=SUSPECT.LST
```

scans just those files listed in SUSPECT.LST. If a pathname is not given the file is assumed to be in the default Toolkit directory.

By default, FindVirus does not scan any compressed and archived files. If you want to scan these files, use the `/UNZIP` and `/PACK` options.

| | |
|---|---|
| `/PACK` | Scans files which have been compressed using the PKLite, LZExe, ICE, Diet and CryptCom utilities. |
| `/UNZIP` | Scans files which have been archived or compressed with ARC, PKZip, ARJ, LZH, PKLite, LZExe, ICE, Diet, and CryptCom utilities. |
| `/NOPACK` | Turns off scanning compressed files (PKLite, LZExe, ICE, Diet, or Cryptcom). This is the default setting. |

For example:

```
FINDVIRU C: /NOPACK /UNZIP
```

enables the scanning of archived files (PKZip, ARJ, ARC and LZH) but not compressed files (PKLite, LZExe, ICE, Diet and CryptCom).

Scanning compressed and archived files may increase scanning time as files have to be decompressed first.

## Scanning boot and partition sectors

By default, FindVirus scans boot and partition sectors on every disk. You can turn these checks off, but this is only recommended if an option is causing a problem; for example, if you are scanning a network drive which does not have a boot sector.

| | |
|---|---|
| `/NOBOOT` | Stops FindVirus scanning the boot and partition sectors of the disk(s) specified. |
| `/NOPART` | Stops FindVirus scanning the partition sector of the disk(s) specified. |

## Producing reports

By default, FindVirus displays a report on the screen when it has finished its scan. A number of additional reporting options are available.

| | |
|---|---|
| `/PRINTOUT` | Directs the report to the default system printer as well as to the screen. |
| `/REPORT=`*`file`* | Directs the report to the specified file as well as to the screen. The `/APPEND` switch appends the report to an existing file. If you only give a filename, the file is created in the default Toolkit directory. If you are running FindVirus from the original write-protected diskette, you must specify a file on the C: drive. |
| `/LOUD` | Provides a more detailed report. As each file is scanned, the result is displayed on the screen. |
| `/BADLIST=`*`file`* | Writes the names of suspect files, together with viruses, to the specified file. If you only give a filename, the file is created in the default Toolkit directory. To save it elsewhere, give a full pathname. |

For example:

```
FINDVIRU C: /REPORT=VIRUS.REP /LOUD
```

scans the C: drive for viruses. As each file is scanned, its name is displayed on the screen. This detailed information is also written to a file called VIRUS.REP in the Toolkit directory.

## Specifying actions

A number of switches can be set to request particular actions during or after a scan.

`/BEEP` Sounds a beep whenever a virus is encountered. By default, one beep is sounded at the end of the scan if any viruses have been detected.

`/ONVIRUS=`*`action`* This switch tells FindVirus what to do if it finds a virus. The two options are:

`/ONVIRUS=HALT` This can only be used if you are running under DOS. The PC hangs and you have to reboot in order to continue.

`/ONVIRUS="`*`message`*`"` If this switch is set, FindVirus displays a message. The message must be in quotation marks and can contain any character except double quotation marks (") and forward slash (/), to a maximum of 40 characters.

For example:

```
FINDVIRUS /LOCAL /ONVIRUS="Virus found. Call PC
Support on 1234"
```

scans all local drives for viruses. If a virus is found, the warning message is output to the screen.

## Network options

If you are using a PC on a network there are some additional options to allow a message to be sent to the supervisor or member of support staff. The default is to send the following message to the network supervisor:

```
<username> : Virus found on workstation!!!
```

where:

*username* is the name of the logged-on user.

The default message and the person to whom it is sent can be changed using the /MSG and /TELL switches.

/MSG="*message*" Sends the specified message to the network supervisor. The message must be in quotes and can contain any character except double quote (") and forward slash (/), to a maximum of 40 characters.

/TELL=*name* Specifies the user to whom the message is sent. The name must be the network identifier of the recipient, such as a network administrator or member of the support staff. The username can be in upper or lower case. You must use this switch in conjunction with /MSG.

For example:

```
FINDVIRU /ALLDRIVES /MSG="Urgent! A virus has
been found" /TELL=DSMITH
```

scans all hard drives, including network drives. If a virus is found, the specified message together with the username of the logged-on user is sent to DSMITH.

Network messages can be prevented if required.

/NOMSG Turns off all network messaging.

## Defining drivers

When scanning, FindVirus uses a virus driver file called FINDVIRU.DRV which contains details of all current viruses. It also checks for an additional driver file called EXTRA.DRV which may contain details of more viruses. If additional drivers are provided by S&S, for example, as an upgrade, you may need to use one of the following switches.

`/DRIVER=`*`file`* Instructs FindVirus to use the named virus driver file instead of FINDVIRU.DRV.

`/EXTRA=`*`file`* Instructs FindVirus to use the named additional driver file instead of EXTRA.DRV.

Extra driver files are available from the S&S Bulletin Board.

## Repairing files

To repair infected files, you can run FindVirus with the `/REPAIR` option.

The Repair button on the user interface provides a straightforward way of repairing files, boot sectors and partition sectors. See Chapter 5, "If you Find a Virus".

`/REPAIR` Runs the repair options. If a virus is found, FindVirus attempts to repair the file. If the virus cannot be removed, the infected file is renamed to prevent accidental use, for example, EXE files are renamed with VXE extensions. Infected boot and partition sectors are also repaired.

`/DELETE` The `/DELETE` switch causes FindVirus to delete any files that cannot be repaired, rather than renaming them. Before deleting the files, FindVirus overwrites

them with zeroes to prevent anyone recovering them with an UNDELETE tool. You can only use `/DELETE` in conjunction with the `/REPAIR` option.

For example:

```
FINDVIRU /LOCAL /REPAIR /DELETE
```

scans all local hard disks for viruses, and attempts to repair any infected files found. If any infected files cannot be recovered, they are deleted. FindVirus prompts for confirmation before deleting each file.

## Heuristic Analysis

This specifies an additional scan for unknown viruses.

| | |
|---|---|
| `/ANALYZE` | Runs the heuristic scanner. |

For more information, see "Heuristic Analysis" on page 78.

## Requesting extended errorlevels

FindVirus returns an errorlevel after running. If you are writing batch files, you can request extended errorlevels, giving more information on errors.

| | |
|---|---|
| `/EXTERROR` | Provides extended errorlevels, as explained in "Errorlevels" on page 90. |

## 7.4 Hints and Tips

### Errorlevels

FindVirus sets an errorlevel each time it runs. When writing batch files, you can use the ERRORLEVEL parameter on the IF command line to determine further actions. See your DOS manual for more information.

The standard errorlevels are as follows:

| Errorlevel | Meaning |
|---|---|
| 255 | Execution interrupted by user. |
| 2 | A virus was found. |
| 1 | A problem was encountered which was not a virus. For example, a file could not be read. |
| 0 | No problems encountered. |

You can request FindVirus to set extended errorlevels by using the `/EXTERROR` switch. These are as follows:

| Errorlevel | Meaning |
|---|---|
| 255 | Execution interrupted by user. |
| 48 | File virus, virus dropper or virus test file found. |
| 47 | Partition sector virus found. |
| 46 | Boot sector virus found. |
| 45 | Virus found in memory. |
| 44 | Trojan found. |
| 22 | Driver file failed checksum. |
| 21 | Driver file not found. |

| Errorlevel | Meaning |
|---|---|
| 20 | Failed integrity check. |
| 11 | Joke program found. |
| 10 | Compressed files found. |
| 1 | A problem was encountered, which was not a virus. For example, a file which could not be read. |
| 0 | No problems encountered. |

## Hard disk device drivers

If your hard disk uses a utility such as Disk Manager, DoubleSpace, SpeedStor, Stacker, SuperStor or Vfeature to access it, you should boot from a diskette that loads the necessary software (usually a device driver) and run FindVirus to scan the C: drive first.

## Speeding up FindVirus

FindVirus uses virtual memory techniques to improve its performance. If you do not have much available memory, the program may have to scan the hard disk twice or more. In this case you can speed up FindVirus by freeing memory, for example by unloading active TSRs. Alternatively, you could run FindVirus from the command line instead of from the user interface.

## Scanning backup files

If you use FastBack or PCTools to make backups, FindVirus might report that the backup diskettes cannot be read. Because of the formatting, DOS cannot read the boot sector or any of the files on these diskettes.

If you have had a virus outbreak, you should assume that any unreadable diskettes are infected, and restore copies from a clean PC as soon as possible.

### False alarms

Very occasionally, FindVirus may report a false alarm, that is, it may report a virus in a clean file. This occurs if the pattern of bytes found in a virus is also found in an uninfected file.

If you are in any doubt, contact your authorized distributor or S&S Technical Support.

### Testing FindVirus

To see how FindVirus behaves if a virus is discovered, you can test the operation of FindVirus. See "Testing VirusGuard" on page 108.

## 7.5 Error messages

This section gives the most common error messages returned by FindVirus, with an explanation of why the error has occurred.

**Cannot execute FINDVIRU.EXE**

There is insufficient memory for FINDVIRU.EXE to load.

**The program has been altered; please replace it with a good copy.**

Changes have occurred to FINDVIRU.EXE. Copy a clean version of the file from the Toolkit diskette.

**Insufficient memory.**

There is not enough memory for FINDVIRU.EXE to execute.

**Bad MESSAGES.DRV**

The file MESSAGES.DRV is missing, or it has been altered. Check that the file is in the same directory as FINDVIRU.EXE or replace it with a good copy from the original Toolkit diskette.

**Bad driver FINDVIRU.DRV**

The driver file FINDVIRU.DRV is missing, or it has been altered. Check that the file is in the same directory as FINDVIRU.EXE or replace it with a good copy from the original Toolkit diskette.

**Unable to store driver file in XMS. Ensure database is always present.**

If the PC has XMS, and if HIMEM.SYS is loaded, FindVirus stores the driver file in XMS. IF HIMEM.SYS is not loaded, FindVirus accesses the driver file on the drive from which the program was run. If you run FindVirus from diskette, and if HIMEM.SYS is not loaded, do not remove the diskette from which FindVirus was run from the drive.

If you want to scan diskettes in the same drive from which you run FindVirus, HIMEM.SYS must be loaded. Otherwise you should run FindVirus from the hard disk.

**This program is more than xx months old**

FindVirus compares the system date with the date of FINDVIRU.DRV. If the difference is six months or more, FindVirus displays the "out-of-date" message. To ensure you are fully protected from new viruses, you should subscribe to the regular upgrade service. See "Registration and upgrades" on page xxix.

# 8. Advanced Virus Prevention

This chapter includes detailed information on using VirusGuard, including running the program from the command line or within batch files.

## 8.1 How VirusGuard works

VirusGuard is a memory-resident program which intercepts viruses, preventing infected files from being executed. It scans each executable file for viruses every time it is opened or executed, and also scans for boot sector and partition sector viruses. If a virus is found, VirusGuard displays a message and sounds an alarm.

VirusGuard consists of three files. GUARD.COM is the memory-resident scanner program, GUARD.DRV is a driver file which contains information on detecting viruses, and MESSAGES.DRV supports messages in different languages.

### Requirements

Installation of VirusGuard is an optional part of the normal DOS or Windows installation. If you have a 386-based PC or above, with extended or expanded memory, VirusGuard has a minimal effect on system performance. You may notice a little extra disk activity as VirusGuard scans files. If you have a 286-based PC or an XT, VirusGuard can run, but you may notice that the PC runs more slowly.

If you have no additional memory, VirusGuard accesses the driver file from the hard disk. It cannot be run from diskette.

Information on installing VirusGuard is given in Chapter 2, "Installing the Toolkit".

## Running VirusGuard

VirusGuard is best run at system start-up. The Toolkit installation procedure adds GUARD to your AUTOEXEC.BAT file. If you install it separately from the rest of the Toolkit, you should add the appropriate line to the AUTOEXEC.BAT. For example:

```
C:\TOOLKIT\GUARD
```

For increased security, include it as near to the start of the file as possible so VirusGuard is loaded before other software.

If GUARD is not included in your AUTOEXEC.BAT, you must run it from the command line each time you start up the PC.

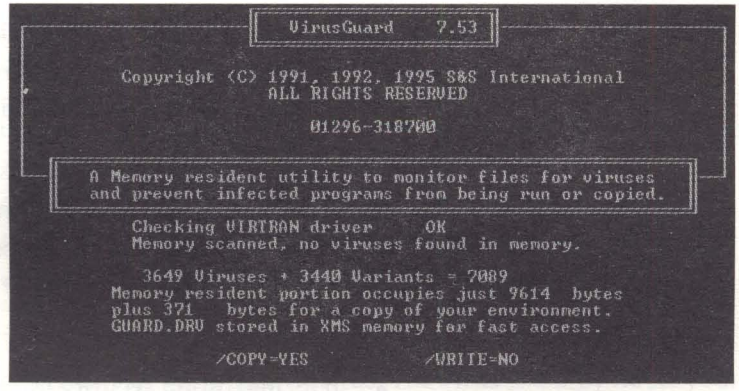
## Use of memory

VirusGuard uses about 9 Kb of conventional memory when resident. This is because it only keeps the scanning program permanently in memory, and reads GUARD.DRV from elsewhere.

If your PC has additional memory installed, VirusGuard uses that for storing the driver. It checks for XMS first and if that is unavailable, it looks for EMS. If neither XMS or EMS is available, it accesses the driver from the hard disk.

VirusGuard itself loads in conventional memory. However, you can load VirusGuard high to reduce its need for base memory. See "Loading high" on page 107.

When VirusGuard is loaded, it displays a screen of the following format:


VirusGuard 7.53
Copyright (C) 1991, 1992, 1995 S&S International
ALL RIGHTS RESERVED
01296-318700
A Memory resident utility to monitor files for viruses
and prevent infected programs from being run or copied.
Checking VIRTRAN driver OK
Memory scanned, no viruses found in memory.
3649 Viruses + 3440 Variants = 7089
Memory resident portion occupies just 9614 bytes
plus 371 bytes for a copy of your environment.
GUARD.DRV stored in XMS memory for fast access.
/COPY=YES /WRITE=NO

This screen includes the following information:

- The VirusGuard version number.
- The results of an initial memory scan.
- The number of viruses that VirusGuard currently scans for.
- How much memory GUARD.COM uses.
- Where GUARD.DRV is stored.
- The current settings of the `/WRITE` and `/COPY` switches. (See "Scanning files when copying or reading" on page 100 and "Scanning files when writing" on page 101.)

## Security levels

When it is first run, VirusGuard scans the PC's memory, the hard disk's boot and partition sectors, the hidden system files and COMMAND.COM.

You can select one of three different security levels when you install VirusGuard, and subsequent scanning depends on the security level set.

- In its **minimum** security mode, VirusGuard scans all executable files before they are run. It also scans executable files copied from diskette and scans all diskettes for boot sector viruses.
- In the **standard** security setting, as well as the minimum scans, VirusGuard scans all executable files as they are copied, not just those that are copied from diskette. This is the default setting.
- In its **maximum** security mode, VirusGuard additionally scans all files before they are written.

Standard security is adequate for most circumstances. To change the security level at any time after installation, see "Changing the security level" on page 106.

## Executable files

File viruses only infect executable files. When scanning executable files, VirusGuard looks for files with the following extensions:

| | |
|---|---|
| APP | EXE |
| BIN | OVL |
| COM | OVR |
| DLL | SCR |
| DOC | SYS |
| DOT | XTP |

## Boot sector scans

VirusGuard scans for boot sector viruses whenever you put a diskette into a drive and access it, even if you only run a DIR command. If a boot sector virus is present, VirusGuard will display a warning.

On most PCs, VirusGuard only scans for boot sector viruses the first time you access the diskette. Subsequent accesses are not scanned unless you have removed the diskette and re-inserted it. However, on some 8088 PCs and XTs, VirusGuard scans every diskette access.

VirusGuard does not stop you accessing a diskette that is infected with a boot sector virus. The virus can only infect your PC if you try to boot the computer from the infected diskette, so it is safe to copy files from the diskette (assuming that the diskette does not contain any file viruses).

If you leave an infected diskette in the A: drive and reboot the PC, VirusGuard cannot prevent infection, because the virus is loaded from the diskette before VirusGuard is run. VirusGuard warns you when it detects an infected diskette, but it cannot physically stop you using it.

## Finding viruses

VirusGuard scans for viruses using the current virus driver. It can find almost all the viruses found by FindVirus. When a virus is found, it will prevent you from running or copying the file in question, and will sound the alarm.

However, there are a few viruses which VirusGuard can detect, but cannot prevent from running. These are some of the more complex polymorphic viruses. WinGuard can stop these viruses before they run, so it is the recommended option under Windows. If one of these is detected, the pop-up alarm is still displayed. You should immediately run FindVirus to locate and identify the virus and remove it.

## 8.2 Running VirusGuard

You can run VirusGuard from the command line or within a batch file with a variety of switches and parameters.

The standard command syntax is:

```
GUARD [switches]
```

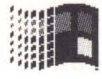
The available switches are discussed in the following sections.

You cannot use any switch more than once on the command line. For example, only the first `/COPY` will have any effect. The switches must be separated by spaces, and they can be typed in upper or lower case.

### Scanning files when copying or reading

By default, VirusGuard scans all executable programs when they are copied or read. The `/COPY=` switch can be used to change this default.

| | |
|---|---|
| `/COPY=NO` | Files are not scanned when they are copied or read, only when they are run. |



This has one important consequence if you runWindows with only VirusGuard loaded, not WinGuard . Then, if you use the `/COPY=NO` switch, Windows applications are not scanned when they are *executed*. This is because Windows runs its applications in a way that bypasses the DOS Execute Program function.

To ensure that Windows applications are scanned when they are run, it is definitely best to use WinGuard; but otherwise, do not use the `/COPY=NO` switch.

If you use the `/COPY=NO` switch, it is possible for an infected file to be copied to your hard disk. However, VirusGuard will warn you if you subsequently try to run the infected program under DOS.

You can also request VirusGuard to scan all files, including data files, whenever they are copied or read.

| | |
|---|---|
| `/COPY=ALL` | Scans all files when they are copied or read, regardless of their extension. |

Scanning all files slows down PC performance during disk accesses and makes minimal difference in the level of security, so it is not recommended for general use.

Also, you can specify that VirusGuard should scan files during read and copy operations whenever files are read or copied from local drives.

| | |
|---|---|
| `/COPY=LOCAL` | Scans files on local drives when they are copied or read |

Alternatively, you can confine read and copy scanning to files that are read or copied from diskette. This gives extra security, particularly since viruses are usually transferred via diskette.

| | |
|---|---|
| `/COPY=FLOPPY` | Scans files on diskette when they are copied or read. |

## Scanning files when writing

By default, VirusGuard does not scan files before they are written. You can use the `/WRITE=` switch to change this default.

| | |
|---|---|
| `/WRITE=YES` | Scans all executable files before they are written. |
| `/WRITE=ALL` | Scans all files before they are written, regardless of extension. |

Scanning all files will slow your PC down during disk accesses and in most circumstances this level of security is unnecessary. You may wish to use this if you have executable files with extensions that would otherwise not be scanned.

You can also restrict VirusGuard to scan files only when they are written to local drives or to diskettes.

`/WRITE=LOCAL` Scans files on local drives when they are copied or read.

`/WRITE=FLOPPY` Scans files on diskette when they are copied or read.

The `/WRITE=` switch does not work when a file is written to a device rather than to a DOS disk. This means that files written to network drives are not scanned by this option, because DOS treats network drives as devices.

## Scanning Windows font files

If you use Windows, you can also scan font files for viruses, although there is only a remote chance of these files being infected. This switch increases the time that Windows takes to load.

`/FON=YES` Scans all files with FON extensions.

For example:

```
GUARD /COPY=FLOPPY /FON=YES
```

scans all files that are read or copied from diskette, and treats all files with FON extensions as executables, in addition to its normal scanning. Most users will find this switch unnecessary.

## Protecting diskettes

You can also use VirusGuard to scan diskettes for an authorization code marked on them by the Author program (see "Marking diskettes with an authorization code" on page 112). Before using this option you must use the Author program to mark all diskettes with a code.

`/CODE="code"` Checks all diskettes for the authorization code marked on the diskette by Author. You must specify the 6-character code which was used when the diskettes were marked.

If you subsequently insert an unauthorized diskette in the drive, the VirusGuard alarm will pop up with the message:

```
A disk which is not authorized in drive x
```

where `x` is the letter of the drive containing the unauthorized diskette.

The `/CODE` switch warns you of unauthorized diskettes but does not prevent their use. If you need to prevent anyone accessing an unauthorized diskette, you should use the `/STRICT` switch in addition to the `/CODE` switch.

For example:

```
GUARD /CODE="A5GE4K" /STRICT
```

This completely prevents access to any diskettes which are not marked with the specified code. It causes the PC to believe that the diskette is unreadable. An error message is displayed, followed by the standard VirusGuard pop-up alarm.

The `/STRICT` switch will prevent you from formatting diskettes, even if they have previously been authorized. The FORMAT program overwrites the authorization code on a diskette. While the format is in progress, the diskette becomes unauthorized and any further access is prevented.

## Location of virus driver

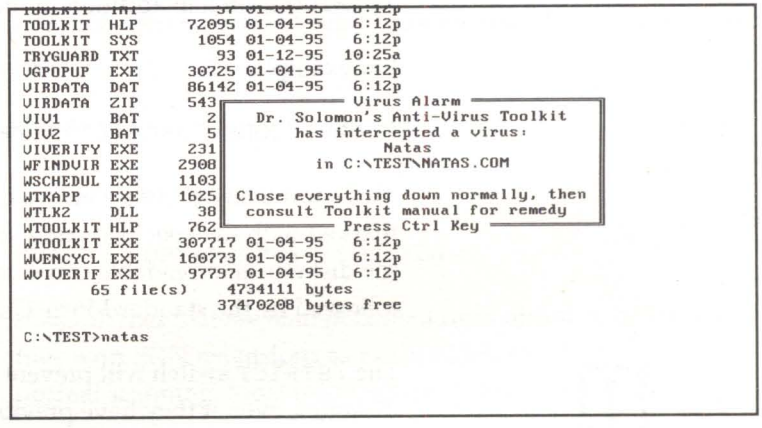
By default, VirusGuard stores the driver file GUARD.DRV in XMS, if it is available. If XMS is unavailable it checks for EMS, and if no additional memory is available the driver is stored on the hard disk. You can force VirusGuard to store the virus driver in a different location, using a command line switch.

`/MODE=EMS` Forces VirusGuard to store the driver in EMS rather than XMS if both are present.

`/MODE=DISK` Forces VirusGuard to store the driver on the hard disk instead of in memory.

## Changing the pop-up message

The standard VirusGuard alarm box is as follows:




The last line of the message can be changed.

`/WARN="message"` Specifies a particular message to appear on the last line of the pop-up alarm box. The message must be enclosed in quotation marks and can contain any character except double quotation marks (") or forward slash characters (/) to a maximum of 36 characters.

For example:

```
GUARD /WARN="ring 1234"
```

## Using VirusGuard on a network

If you are using a Novell NetWare network, you can configure VirusGuard to send a message to another person whenever an alarm occurs. The default is to send the following message to the network supervisor:

"*username* has had a VirusGuard alarm"

To enable this, you must use the /NET=YES switch.

/NET=YES — Sends the default message to the network supervisor if a virus is detected on any workstation.

The default message and the person to whom it is sent can be changed using the /TELL and /NLRT switches.

/TELL=*username* — Specifies the user to whom VirusGuard sends messages, usually the supervisor or member of the support staff. The username must be a valid network identifier. It can be entered in upper or lower case and should not be enclosed in quotation marks.

If you specify a user name with /TELL=, you do not need to use the /NET=YES option.

/NLRT="*message*" — Allows you to specify a particular message. The message must be in quotation marks and can contain any character except double quotation marks (") and forward slash (/), to a maximum of 40 characters.

When the specified message is sent, it is added to the name of the user logged on at the workstation where the alarm occurs.

If you specify a message using /NLRT=, you do not need to use the /NET=YES option.

For example:

```
GUARD /WARN="Virus alert! message sent to PC
Support" /TELL=PCSUPP /NLRT="Urgent - Virus
detected by VirusGuard"
```

If a virus is detected, the specified message is sent to user PCSUPP. The PC user will still see the VirusGuard pop-up alarm, and the last line of the pop-up message will indicate that a message has been sent to PC Support.

If the message cannot be sent for any reason, for example if the recipient is not logged on to the network, VirusGuard continues as if the network messaging facility had not been switched on. For further information on running VirusGuard on a network, see Chapter 12, "Using the Toolkit on a Network".

## 8.3 Hints and Tips

### Changing the security level

If you need more or less security at any time, you can change VirusGuard's security level by running GUARD with certain switches.

To set VirusGuard to maximum security, use the command:

```
GUARD /COPY=ALL /WRITE=ALL
```

This scans files when they are copied, read or written.

For standard security, run VirusGuard with no /COPY or /WRITE switches.

To set VirusGuard to minimum security, use the command:

```
GUARD /COPY=FLOPPY /WRITE=NO
```

This scans for viruses when files are copied and read from diskette. No scanning is performed when files are written.

If GUARD.COM is included in your AUTOEXEC.BAT file, you can edit the parameters using a text editor or a word processor. When you run VirusGuard it confirms the status of the `/COPY` and `/WRITE` switches, as shown on page 97. Virus Guard is not reinstalled.

## Loading high

You may find it an advantage to load VirusGuard into the upper memory area, rather than the conventional memory area, leaving more space to run applications. To do this, you must have additional memory installed, and you must be running one of the following:

- MS-DOS 5.0 or higher.
- DR-DOS 5.0 or higher.
- PC-DOS 5.0 or higher.
- QEMM.
- 386MAX.

You must also have configured the upper memory area in your CONFIG.SYS file. Your operating system user guide will tell you how to do this.

If you are using MS-DOS, DR-DOS or PC-DOS, load VirusGuard using the LOADHIGH or LH command. Run the following command in the Toolkit directory:

```
LH GUARD
```

Alternatively, insert the following command into your AUTOEXEC.BAT file:

```
LH C:\TOOLKIT\GUARD
```

If you are running QEMM or 386MAX memory management software, see the relevant documentation for information on loading high.

## 8.4 Testing VirusGuard

### File virus test

To enable you to test VirusGuard and see how it behaves when it detects a file virus, you can set up a test file.

Follow these steps:

1. Before the test, make sure that VirusGuard is loaded and that you do not have the `/COPY=NO` or the `/WRITE=ALL` switches on, as these interfere with the test.

2. Use a text editor or word processor to create a file called `TRYGUARD.DOC`.

3. Enter the first nine characters of the file as:

   ZQZXJVBVT

   These characters must be in upper case.

4. If you want to test FindVirus as well, ensure that there are at least 50 characters in the file.

5. Save the file as an ASCII text file. Do not save it as a formatted document, as this would insert extra characters at the beginning of the file and stop it from being recognized by VirusGuard.

   If VirusGuard is set up with the `/WRITE=ALL` switch, you will not be able to save the file.

6. Rename the file with the following command from the DOS prompt:

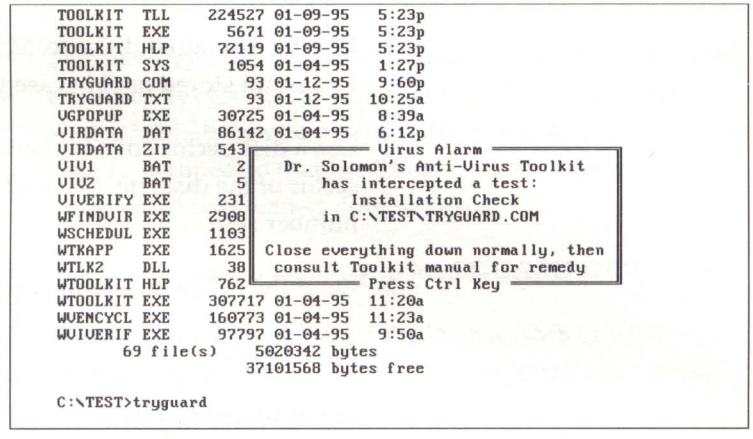
   ```
   REN TRYGUARD.DOC TRYGUARD.COM
   ```

   The COM extension will ensure that VirusGuard scans the file as though it were an executable file.

7. To run the test, enter the command:

   ```
   COPY TRYGUARD.COM NUL
   ```

   DOS attempts to copy the test file, an action which is checked by VirusGuard. The alarm pops up and reports the test as follows:




If the file is at least 50 characters long, it will also be found if you run FindVirus.

VirusGuard would also intercept the file if you tried to run it as a program. However, as the test file is not executable, it would not run even if VirusGuard was not resident, and may cause the PC to hang.

When you have finished the test, delete the file or rename the file giving it a DOC file extension so that FindVirus doesn't give someone a shock later on.

## Boot sector virus test

You can perform a similar test on a diskette to see what happens when VirusGuard finds a boot sector virus.

For this test, you need to know how to use a disk sector editor, such as DOS DEBUG. If you are not familiar with tools such as these, you should not attempt to do this.

1. Insert a formatted diskette. Make sure there is nothing important stored on it in case you make a mistake.
2. Use a disk sector editor to write to byte 64 (40H) in the boot sector of the diskette. Remember that the first byte is number zero.
3. Enter the following characters, without the quotation marks:

   "Confidence"

   In hexadecimal, this is:

   43 6F 6E 66 69 64 65 6E 63 65
4. Remove the diskette, then re-insert it and type `DIR` to list the files on the diskette.
5. The VirusGuard pop-up alarm appears, reporting an Installation Check. If you run FindVirus, it will also report the test.

When you have completed the test, reformat the diskette to avoid giving someone a shock later on.

## 8.5 VirusGuard error messages

This section gives the most common error messages returned by VirusGuard, with an explanation of why the error has occurred.

**VirusGuard driver access error! Scan incomplete.**

This message is displayed if VirusGuard is unable to access its driver. Typically, this occurs if VirusGuard has been loaded initially from a network drive which, after login, has been re-mapped so that the directory from which VirusGuard was loaded does not exist.

**ERROR - not enough memory to load GUARD.DRV.**

This message is displayed if the PC has XMS or EMS memory, but not enough to store VirusGuard's driver file (GUARD.DRV).

**ERROR - Can't find or read GUARD.DRV - VIRUSGUARD NOT INSTALLED.**

GUARD.DRV is not in the same directory from which VirusGuard was loaded; or VirusGuard is unable to read GUARD.DRV.

**ERROR - VirusGuard must not be run from a floppy disk. Install the program and drivers on a hard disk and run from there.**

VirusGuard cannot be run from a diskette drive.

**CHECKSUM TEST FAILED - TAMPERING DETECTED - VIRUSGUARD NOT INSTALLED.**

GUARD.COM has been altered. Copy a clean version of the file from the Toolkit diskette.

**The GUARD.DRV database is xx months old . . . .**

VirusGuard compares the system date with the date of GUARD.DRV (the virus driver). If the difference is six months or more, the "out-of-date" message appears.

To ensure that you are fully protected from new viruses, you should subscribe to the regular upgrade service. See "Registration and upgrades" on page xxix.

## 8.6 Marking diskettes with an authorization code

If you need extra security on your PC you can use the Author program to mark diskettes with an authorization code. You can then use VirusGuard to check diskettes for the correct code as well as for viruses. If you insert a diskette with the wrong code, or without a code, the alarm is sounded and a warning appears. This will help discourage the use of diskettes which have not been virus-checked and authorized.

This feature can be used as a handy reminder. If you authorize all diskettes, any diskette that comes in from outside triggers a warning. It can then be checked for viruses on a sheep-dip PC.

### How Author works

To use the authorization facility, all the diskettes you use must be marked with the authorization code, and VirusGuard must be installed with the `/CODE` option. See "Protecting diskettes" on page 102.

By default, VirusGuard does not prevent you from using unauthorized diskettes; it simply sets off the alarm and displays a warning. You can override the warning, for example, to install software from write-protected diskettes.

If you reformat an authorized diskette, you will need to authorize it again.

To prevent anyone from accessing unauthorized diskettes, they can be made completely inaccessible by using the `/STRICT` switch.

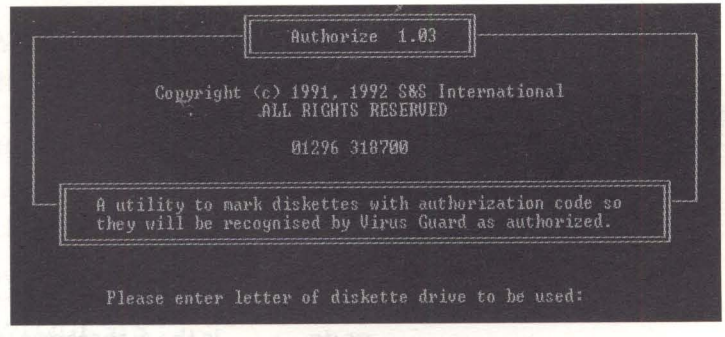
Some backup programs reformat diskettes when they back up the files, in which case the diskettes will lose their authorization. It may not be possible to reauthorize such diskettes since the backup software may interfere with the VirusGuard authorization feature. You will have to choose either to use different backup software or not to use the authorization feature.

## Running Author

You must run Author from the DOS command line. It is not available on the menu.

If you enter `AUTHOR` with no parameters, you are prompted for the authorization details. Follow the steps below:

1. Insert a write-enabled diskette that you wish to authorize in the drive.
2. Change to the Toolkit directory. Type `AUTHOR` and press ↵. The following screen is displayed:


Authorize 1.03
Copyright (c) 1991, 1992 S&S International
ALL RIGHTS RESERVED
01296 318700
A utility to mark diskettes with authorization code so they will be recognised by Virus Guard as authorized.
Please enter letter of diskette drive to be used:

3. Enter the appropriate diskette drive letter and press ↵.

4. You are then prompted for an authorization code. Type in six characters, using any characters except quotation marks (") or forward slashes (/). Then press ↵.

   The program does not distinguish between uppercase and lowercase characters.

   If you enter less than six characters, the remaining characters are automatically written as spaces. It is more secure to specify all six characters.

5. To authorize more than one diskette in the same drive, remove the first diskette and replace it with the next. Then press ↵.

6. If you want to authorize diskettes in a different drive, press the new letter instead of ↵ when prompted.

7. Press Esc to return to the system prompt when you have authorized all the diskettes.

You can authorize as many diskettes as you like by inserting a new one and pressing ↵. To change to a different drive, press the appropriate drive letter.

Press Esc to return to the system prompt when you have authorized all diskettes.

Alternatively, you can provide all the information on the command line. The command then has the following syntax:

```
AUTHOR /DISK=drive /CODE="code"
```

where:

| | |
|---|---|
| *drive* | is the diskette drive in use (without the colon). |
| *code* | is the 6-character authorization code. The code must be contained in quotation marks. |

For example:

```
AUTHOR /DISK=A /CODE="P7KG5R"
```

# 9. Advanced Virus Checking

This chapter provides detailed information on using ViVerify, including running the program from the command line or from within batch files.

## 9.1 How ViVerify works

ViVerify is a checksummer which is able to detect changes in executable files that may have been caused by a virus infection. ViVerify works by calculating a unique fingerprint for each file. This fingerprint is then recalculated when required, to check if there have been any changes.

### Executable files

ViVerify only checks for changes in executable files. By default, it checks files with the following extensions:

| | |
|---|---|
| APP | FON |
| BAT | OV? |
| BIN | SYS |
| COM | XTP |
| DLL | 386 |
| EXE | |

Most executable files do not change, so any variation in the checksum may be an early warning of a virus infection. Occasionally, though, you may have an executable file that does change, or a data file that has one of the above file extensions. Specific individual files of this sort can be excluded from the checks. The following files are excluded by default:

CONFIG.SYS
WPQUE.SYS
WPSYSD.SYS
BOOTCONF.SYS
TELIX.FON

ViVerify also checks boot and partition sectors for changes.

## Encryption algorithms

To create unique fingerprints (checksums) which cannot be detected by the virus, ViVerify uses an encryption algorithm.

The default algorithm used is the CCITT Cyclic Redundancy Check (CRC). This incorporates a user-specified keyword to increase security, and checks the files rapidly.

The Size algorithm calculates fingerprints based only on the size of the file. This is very quick, but can be fooled, or "spoofed", by some viruses.

The Checksum algorithm calculates fingerprints as a whole sum of the bytes checked in the files. It also incorporates the user-specified keyword.

The DES algorithm uses the standard Data Encryption Standard (DES) algorithm. This is the most secure option, but requires lengthy calculations, so it can slow down the checking.

## Checking speed

By default, ViVerify speeds up the checking process by checking only the first and last 4 Kb of each file. This is known as turbo mode. If you need particularly high security, you can turn turbo mode off, allowing ViVerify to check the entire file.

However, it is very unlikely that a virus will infect a file without making changes to the beginning or end of the file.

To speed up checking further, ViVerify normally checks every fifth byte in a file since it is difficult for a virus to infect a file without modifying at least one of the bytes checked by ViVerify. You can change this if you need greater security or faster checking on your system.

### Running ViVerify

There are three stages to running ViVerify:

- Create a list of the files to be checked for changes.
- Calculate fingerprints for these files.
- When required, recalculate the fingerprints to check for changes.

## 9.2 Running ViVerify from the user interface

You can run ViVerify from the Toolkit user interface in the following ways:

- By selecting the Check for Changes option on the main screen.
- By selecting Check for Changes from the Scan menu.

These options are explained in detail in Chapter 5. See "Checking for changes - ViVerify" on page 57.

## 9.3 Running ViVerify from the command line

You can run ViVerify from the command line, or within a batch file, with a number of switches.

The standard command syntax is:

```
VIVERIFY function [switches]
```

The available functions are as follows:

| | |
|---|---|
| `FILELIST` | Make a list of the files to check. |
| `MAKEPRINT` | Calculate the fingerprints for the listed files. |
| `CHECKPRINT` | Check the files in the list for changes. |

| | |
|---|---|
| `AUTOMAKE` | Perform `FILELIST` and `MAKEPRINT` functions in one operation. Note that this is not available in the Windows version. |

The available switches are explained in detail in the following sections. You cannot use any switch more than once on the command line. The switches must be separated by spaces, and they can be typed in upper or lower case.

## Checking specific drives

When using any function, you should specify the drive(s) to be checked using the `/D=` switch.

| | |
|---|---|
| `/D=`*`drive`* | Indicates one or more drives to be checked. |

Enter one or more of the identifying letters without spaces between them. Do not enter the colon. For example:

```
VIVERIFY /D=CD
```

will check the C: and D: drives.

You can also use a wildcard. For example:

```
VIVERIFY /D=*
```

will check all local drives.

## Defining files to be checked

By default, ViVerify checks all executable files on the selected drive. When you use the FILELIST function, it will create a file containing a list of all the files to be checked. This file, normally called FILES.VVL, is subsequently used by the MAKEPRINT and CHECKPRINT functions.

If you want to check the contents of different drives separately, you can create separate file lists for each drive. In these circumstances, you should define particular file lists to be used, rather than using the default filename.

`/FL=file` With the `FILELIST` function, creates a file of the specified name to hold the list of files to be checked. With the AUTOMAKE, MAKEPRINT, and CHECKPRINT functions, checks all files listed in file.

For example:

```
VIVERIFY FILELIST /D=C /FL=C_FILES.VVL
```

creates a list of all the executable files on the C drive that are to be checked, and saves the list in a file called C_FILES.VVL in the default Toolkit directory.

## Specifying a fingerprint file

When you use the MAKEPRINT or AUTOPRINT functions, the fingerprints created are stored in a file for future use by CHECKPRINT. By default, this file is called FINGERP.VVF. If you want to check the contents of different drives separately, you can create separate fingerprint files for each drive.

`/FS=file` Specifies a particular file in which the
`/FPRINT=file` fingerprints are saved.

You can use either the `/FS` switch or the `/FPRINT` switch; there is no difference.

For example:

```
VIVERIFY MAKEPRINT /FL=C_FILES.VVL
/FS=C_FPRINT.VVL
```

creates fingerprints for all files listed in the file C_FILES.VVL. (This assumes that the FILELIST function has already been run to create this list.) The fingerprints are saved in a file called C_FPRINT.VVL in the default Toolkit directory.

Remember that when you subsequently check the fingerprints using the CHECKPRINT function you must use the same file that you specified when you created the fingerprints.

## Excluding files

ViVerify allows you to specify individual files which are not to be checked, for example executable files which you know are likely to change legitimately.

When it runs, ViVerify checks for a file called EXCLUDE.VVX in the Toolkit directory. If you have files that are likely to change legitimately, you can add them to EXCLUDE.VVX.

Alternatively, you can create a file containing the names of the files you want to exclude. This should be an ASCII file containing names of files that are not be checked. File extensions should be included. If you do not provide a pathname, all occurrences of the file will be excluded.

If you use a file other than EXCLUDE.VVX, you must specify it using the `/EXCLUDE` option.

| | |
|---|---|
| `/EXCLUDE=`*`file`* | Excludes from the checking process all files listed in the specified file. |

Some network system files are inaccessible over a network. To ensure that these are excluded from the file list, the `/NETVOL` switch should be used.

| | |
|---|---|
| `/NETVOL` | Excludes all network system files inaccessible over a network. |

## Checking boot and partition sectors

By default, ViVerify checks the boot and partition sectors of every disk it examines. You can turn these checks off, but this is not recommended unless an option is causing a problem. For example, if you are checking a network drive which does not have a boot sector.

| | |
|---|---|
| `/NOBOOT` | Stops ViVerify from checking the boot sectors. |
| `/NOPART` | Stops ViVerify from checking partition sectors. |

## Specifying a keyword

When you use the MAKEPRINT or AUTOMAKE functions, you must specify a keyword to be used in the fingerprinting algorithm (unless you are using the Size algorithm, which does not use a keyword.)

When you subsequently use the CHECKPRINT function on the same list of files, you must give the same keyword as a parameter.

`/X=keyword` Specifies a keyword to be used when creating or checking fingerprints. The keyword must be at least eight alpha-numeric characters.

For example:

```
VIVERIFY AUTOMAKE /D=C /X=D5R2L0H7
```

will create a list of executable files on the C drive to be checked, and will create fingerprints for these listed files, incorporating the user-specified keyword.

## Varying the checking speed and security

If you need a particularly high level of security, you can turn off turbo mode, allowing ViVerify to check the entire file instead of just the first and last 4 Kb.

`/NT` Turns off turbo mode.

ViVerify normally checks every fifth byte in each file, which is sufficient for most users. You can set the program up to check more bytes, to provide greater security, or fewer bytes, for faster checking.

`/N=n` Checks the nth byte of each file.

## Specifying an algorithm

By default, ViVerify calculates fingerprints using the CCITT Cyclic Redundancy Check algorithm. This is suitable for most users, but you can specify a different algorithm if you particularly need greater security or increased checking speed.

| | |
|---|---|
| `/SIZES` | Calculates fingerprints based on the file size. |
| `/CRC` | Uses the CCITT CRC algorithm (default). |
| `/WHOLESUM` | Calculates fingerprints as a whole sum of the bytes checked in the file. |
| `/DES` | Uses the Data Encyption Standard algorithm. |

## Defining actions

You can configure ViVerify to beep when it finds a changed file.

| | |
|---|---|
| `/BEEP` | Beep when a changed file is found. |
| `/BIGBEEP` | Beep loudly when a changed file is found. |

## Producing reports

By default, ViVerify displays a report on the screen when you run the CHECKPRINT function. You can configure ViVerify to wait for a key to be pressed after the report is displayed.

| | |
|---|---|
| `/HOLDKEY` | Wait for a keystroke after displaying the report. |

You can also direct the report to a named file, to the default system printer or to both. You can specify whether the output appears in full or in a shortened form.

| | |
|---|---|
| `/PRINTOUT` | Directs the report to the default system printer as well as to the screen. |

| | |
|---|---|
| `/REPORT=`*`file`* | Directs the report to the specified file as well as to the screen. |
| `/LOUD` | Provides a more detailed report. As each file is checked, its name is displayed on the screen. |
| `/QUIET` | Produces a report in a shortened form. |

For example:

```
VIVERIFY CHECKPRINT /D=C /X=D5R2L0H7 /PRINTOUT
/LOUD
```

will recalculate fingerprints for executable files on the C drive, using the specified keyword in the encryption algorithm. As each file is checked for changes, its name is displayed on the screen, and the report is also sent to the default printer.

## Extended errorlevels

ViVerify returns an errorlevel when it runs. You can request more detailed errorlevels for use in batch files if required. See "Errorlevels" on page 124.

| | |
|---|---|
| `/EXTERROR` | Provide extended errorlevels. |

## Producing a list of suspect files

A list of changed files can be produced and written to a file. The contents of this file can then be checked by FindVirus, using the `/CHECKLIST` option. See "Scanning files and subdirectories" on page 83.

| | |
|---|---|
| `/BADLIST=`*`file`* | Writes a list of suspect files to the specified file. If you give just a filename, the file is created in the Toolkit directory. Alternatively, you can give a full path. |

## Using anti-stealth measures

| | |
|---|---|
| `/ASM` | Use Anti-Stealth Methodology. See "Anti-stealth measures" on page 132 for more information. |

## Errorlevels

ViVerify sets an errorlevel when the CHECKPRINT function is used. When writing batch files, you can use the ERRORLEVEL parameter on the IF command line to determine further actions. See your DOS manual for more information.

The standard errorlevels are as follows:

| Errorlevel | Meaning |
|---|---|
| 255 | Execution interrupted by user. |
| 2 | An executable file has been changed. |
| 1 | A problem was encountered which was not a virus. For example, a file could not be read. |
| 0 | No problems encountered. |

When the `/EXTERROR` switch is set, ViVerify sets the following extended errorlevels:

| Errorlevel | Meaning |
|---|---|
| 255 | Execution interrupted by user. |
| 4 | Files have been deleted. |
| 3 | Invalid entry in fingerprint file. |
| 2 | An executable file has been changed. |
| 1 | File exists but could not be checked. |
| 0 | No problems encountered. |

# 10. Additional Tools

This chapter includes information on additional tools available to the more technical user: GuardMem, Inspect Disk, Inspect File and Inspect Memory.

## 10.1 Checking memory - GuardMem

A large number of viruses are memory-resident. The best way to avoid and detect memory-resident viruses is to cold boot your PC from a clean, write-protected system diskette and then run FindVirus from diskette. However, as this is not always practical, memory-checking facilities are included as part of the Toolkit.

The PC's memory is checked for viruses automatically whenever you start up the DOS or Windows Toolkit. Other programs in the Toolkit also check memory before running.

An additional memory-checking tool, GuardMem, is provided to allow you to run extra memory checks at other times.

GuardMem scans the PC's memory for known memory-resident viruses. It uses a driver called MEM.DRV which is updated whenever you upgrade the Toolkit.

To ensure memory is checked for viruses, MEM.DRV and GUARDMEM.COM must be in the same directory as other Toolkit programs.

To run GuardMem from the main menu, select Check memory from the Scan drop-down menu.

To run GuardMem from the command line or within a batch file, change to the Toolkit directory and enter the command:

`GUARDMEM` and press ↵.

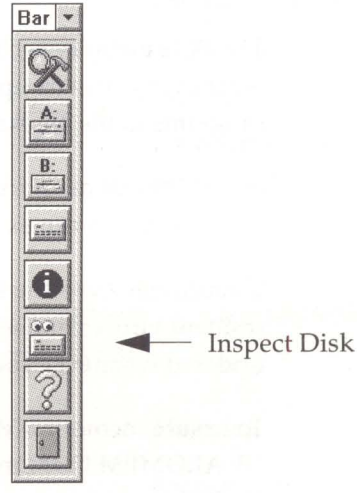
There are no switches.

## 10.2 Examining disks - Inspect Disk

Inspect Disk enables you to examine hard disks and diskettes at a low level. It is safe to use because no data is written to the disk. However, to make the best use of Inspect Disk you need to be familiar with the content and structure of disks.

Inspect Disk allows you to examine the boot sectors of diskettes and the partition and boot sectors of hard disks. Suspect code in these areas may indicate a virus infection.

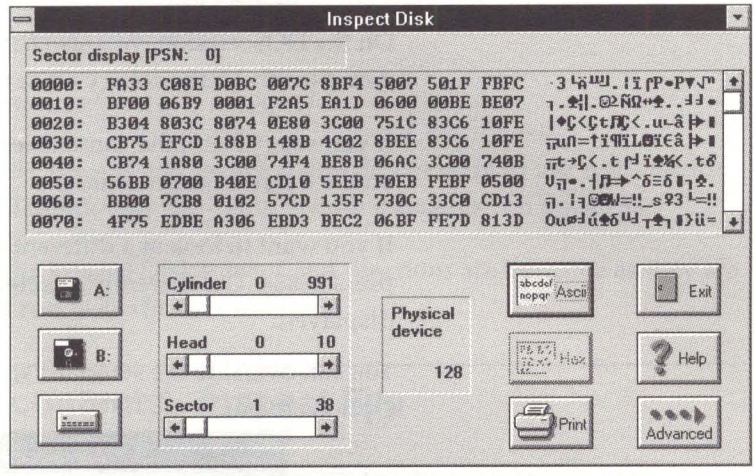
You can run Inspect Disk from the command line or from the menu. If you are using the Windows version of the Toolkit, you can also select Inspect Disk from the toolbar by selecting the appropriate icon:




### Running Inspect disk from the user interface

To examine disks from the menu, select Inspect disk from the Advanced menu.

A screen of the following format is displayed:


Inspect Disk
Sector display [PSN: 0]
0000: FA33 C08E D0BC 007C 8BF4 5007 501F FBFC
0010: BF00 06B9 0001 F2A5 EA1D 0600 00BE BE07
0020: B304 803C 8074 0E80 3C00 751C 83C6 10FE
0030: CB75 EFCD 188B 148B 4C02 8BEE 83C6 10FE
0040: CB74 1A80 3C00 74F4 BE8B 06AC 3C00 740B
0050: 56BB 0700 B40E CD10 5EEB F0EB FEBF 0500
0060: BB00 7CB8 0102 57CD 135F 730C 33C0 CD13
0070: 4F75 EDBE A306 EBD3 BEC2 06BF FE7D 813D
A:
B:
Cylinder 0 991
Head 0 10
Sector 1 38
Physical device
128
Ascii
Hex
Print
Exit
Help
Advanced

Select the drive you want to check from the buttons on the left. Inspect Disk detects which disk drives are installed, and you can select the appropriate drive from those displayed.

If you only have one physical hard drive, it will be shown as a single drive even if it is divided into a number of logical drives. Drives A: and B: refer to physical devices 0 and 1.

If you have more than one physical hard disk, you can only select the first drive from this screen. Use the Advanced option screen to choose other hard disks.

You can navigate around the disk using the Cylinder, Head and Sector scrollbars. If you are using the DOS version of the Toolkit, you can also enter the required values directly. The numbers at the right of each scrollbar indicate the maximum values allowed.

On a hard disk the partition sector is usually at cylinder 0, head 0, sector 1, and the DOS boot sector is usually at cylinder 0, head 1, sector 1. On a diskette, the boot sector is normally at cylinder 0, head 0, sector 1.

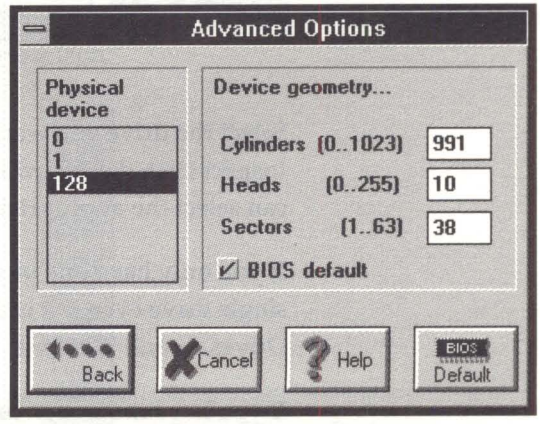
You can choose between displaying the disk contents as ASCII or as hexadecimal.

On the DOS version, you also have the option of switching Anti-Stealth Methodology on or off.

If you select Print, the contents of the current sector are printed on the default system printer.

If you want to look at a different diskette, simply swap it and press Space. The currently selected sector on the new diskette is displayed.

You can override the standard settings using the Advanced Options menu:




The options available are:

Physical device — Lists the physical devices available. Device 0 is drive A:, device 1 is drive B: and the available hard disks are those numbered 128. and above.

Device geometry — The normal maximum values are read from the BIOS when Inspect Disk is started, but you can override the default settings if necessary.

BIOS default — This sets the cylinder, heads and sectors back to the standard BIOS settings.

### Running Inspect Disk from the command line

If you run Inspect Disk from the command line, it has the following syntax:

```
TOOLKIT /ID [/NOASM]
```

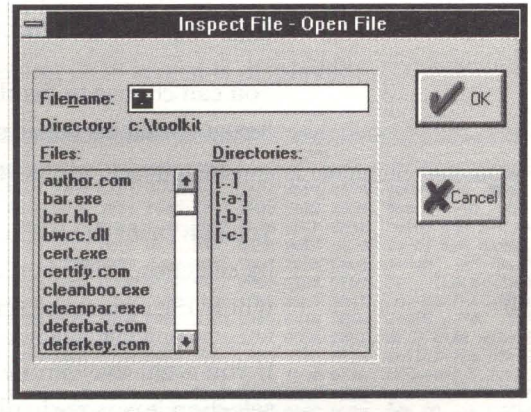
Use the `/NOASM` switch if you do not want to use Anti-Stealth Methodology. See "Anti-stealth measures" on page 132.

The Inspect Disk screens and functions are the same as they are if run from the user interface.

## 10.3 Examining file contents - Inspect File

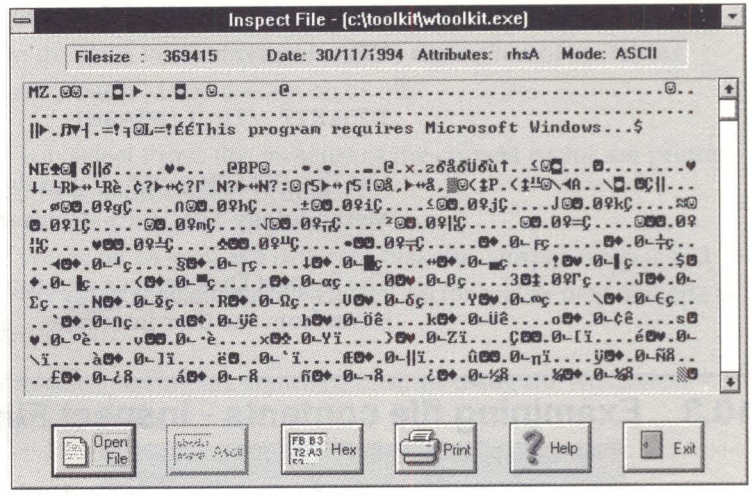
Inspect File enables you to display the contents of a file in either ASCII or hexadecimal to check the effects of a virus. This tool is only available from the user interface.

Select Inspect File from the Advanced menu. The following dialog box is displayed:




Select the file you want to examine and select OK.

The file contents are displayed as follows:




The contents of the file are displayed on the screen. The size of the file, the date it was last changed and its attributes are displayed at the top of the screen.

You can use the scroll bars, the ↓ and ↑ keys, or Pg up and Pg dn keys to scroll through the display if necessary.

You can choose to display the file contents in ASCII or in hexadecimal by selecting the appropriate button. ASCII text is unformatted to allow special characters to be displayed.

You can print the file contents in the currently selected format by selecting Print. You can then choose whether to print the whole file or just the screen display.

If you want to examine another file, select Open File. The file selection box is re-displayed.

## 10.4 Examining memory - Inspect Memory

Inspect Memory enables you to display the contents of the first megabyte of the PC's memory to check for the effects of a virus. This tool is only available from the user interface.

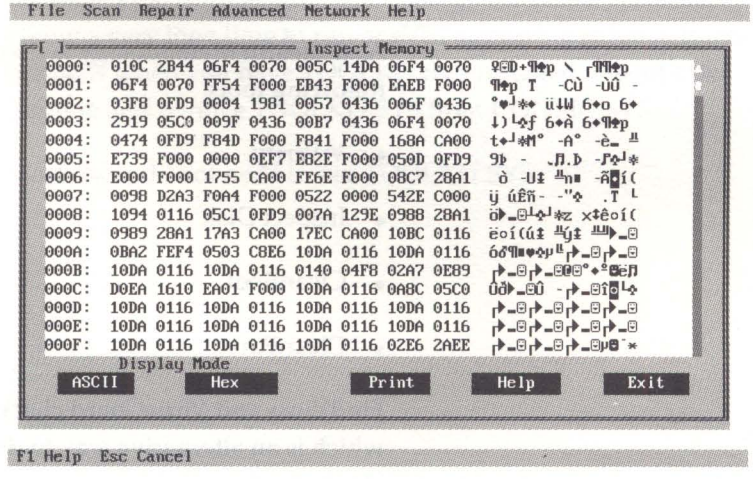
Users who are not experienced with the way that viruses work are unlikely to find Inspect Memory useful.

To run Inspect Memory, select Inspect Memory from the Advanced menu.

If you are running the Windows version of the Toolkit, note that Inspect Memory has to run in real mode. This is because the memory management features of 286 processors and above may prevent Inspect Memory from accessing memory. Therefore Inspect Memory switches to DOS while it runs, and returns to Windows afterwards.

If you are running under Windows, a message appears reminding you that a DOS program must be run. In order to run Inspect Memory, Windows then opens a DOS window.

The following DOS screen is displayed:



You can choose to display the memory contents in ASCII or in hexadecimal. ASCII text is unformatted to allow special characters to be displayed.

You can use the scroll bars, the ↓ and ↑ keys, or Pg up and Pg dn keys to scroll through the display if necessary.

You can print the file contents in the currently selected format by selecting Print.

## 10.5 Anti-stealth measures

Stealth viruses interfere with the DOS and BIOS interrupts to remain hidden.

The best way of dealing with stealth viruses is to cold boot the PC from a clean, write-protected DOS system diskette, and then run FindVirus from diskette before running any executable files. However, this is inconvenient in normal use, so the Toolkit includes special measures to detect and identify viruses using stealth.

It can detect boot sector viruses that use stealth, such as Joshi and Brain, and file viruses that use stealth such as Tequila and Zero-Bug.

Anti-Stealth Methodology is used in the DOS versions of the following tools:

- ViVerify
- Inspect Disk
- CleanBoot
- CleanPart

FindVirus and VirusGuard check memory for known viruses, which is an alternative way to defeat stealth.

In its default setting, ViVerify does not use the Anti-Stealth Methodology. You can turn it on by running them with the `/ASM` switch.

Inspect Disk, CleanBoot and CleanPart use the Anti-Stealth Methodology by default. In this case you can turn them off by using the `/NOASM` switch. You can also turn off the anti-stealth checking for the entire Toolkit by running the command as follows:

```
TOOLKIT /NOASM
```

An additional tool is supplied to enable the use of ASM from system boot-up. TOOLKIT.SYS is a device driver incorporating Anti-Stealth Methodology, which you can install in your CONFIG.SYS file.

Use a text editor or word processor to edit CONFIG.SYS, adding the following line to the end of the file.

```
DEVICE=C:\TOOLKIT\TOOLKIT.SYS
```

This increases the anti-stealth abilities built into the various tools in the Toolkit. It can deal with very well-concealed viruses, such as Frodo and Fish6.

On some PCs, Anti-Stealth Methodology can cause problems by taking a very long time to run or even appearing to hang. If this happens when you have TOOLKIT.SYS installed, reboot from diskette and remove TOOLKIT.SYS from CONFIG.SYS.

Most users do not need to use TOOLKIT.SYS.

# 11. Virus Repair and Removal

The Toolkit user interface includes a straightforward single-button facility for repairing infected files, boot sectors and partition sectors. See Chapter 6, "If You Find a Virus" for more information.

This chapter describes alternative methods of repair, using FindVirus, CleanBoot and CleanPart separately to repair infected files and replace infected boot sectors and partition sectors.

## 11.1 Introduction

If one of the Toolkit programs reports a virus, follow these steps:

1. Don't panic.
2. Save everything you are working on before closing down the PC as normal.
3. Cold boot the PC from a clean, write-protected, DOS system diskette. You should always power off the PC as some viruses can survive a warm reboot.
4. If VirusGuard has reported a virus, or if ViVerify has reported changes to executable files, run FindVirus. This will name any virus present and identify the infected files, boot sectors or partition sectors.

There are a number of repair methods. The simplest is to select the Repair button on the user interface. This option runs FindVirus with the Repair option to fix infected files, diskette boot sectors and hard disk partition sectors.

This option is described in Chapter 6, "If You Find a Virus".

## 11.2 Repairing drives

You can use FindVirus to repair infected drives, including infected files, boot sectors and partition sectors. It can be run from the user interface or from the command line.

It is always more secure to cold boot the PC and run FindVirus from a write-protected diskette.

### Repairing drives from the user interface

To repair drives from the user interface:

1. Select Repair drive from the Repair menu. The following screen is displayed:

2. The settings and options are as follows:

| | |
|---|---|
| Report to | A report of the repair process is displayed on the screen. In addition, you can direct the report to a file, to a printer, or both. |

| | |
|---|---|
| Drives | Select the drives you want to scan. Choose Local to scan all the hard drives on your PC. Select Network to scan all network drives. Select Clear to clear any selections you have made. |
| If file not repairable | By default, if a file cannot be repaired, FindVirus renames it, with the first letter of the file extension being changed to a V, to prevent someone from running it accidentally. For example, FORMAT.COM is changed to FORMAT.VOM.<br><br>If you set the Delete infected files option, FindVirus will delete any files that cannot be repaired. |

Files are overwritten before deletion to ensure that they cannot be recovered by an Undelete program.

3. When all the settings are correct, select Repair. FindVirus scans the specified drives and attempt to repair any infected files found. If boot and partition sectors are infected, they are replaced with clean copies.

When FindVirus is run with the Repair option it scans all files, including data files. This is in case an executable file has been renamed with a different file extension. It also scans files that have been compressed or archived using PKLite, ARC, PKZip, ICE, LZExe, Diet, LZH, CryptCom or ARJ.

FindVirus produces a report detailing the action taken. If files cannot be repaired, you must restore the original clean copies from backups.

## Repairing drives from the command line

If you run the FindVirus repair option from the command line, it has the following syntax:

```
FINDVIRU drive /REPAIR [/DELETE]
```

You must specify the drive to be scanned, either by including the drive on the command line or by using one of the `/D`, `/LOCAL` or `/ALLDRIVES` switches.

When FindVirus is run with the Repair option it scans all files, including data files. This is in case an executable file has been renamed with a different file extension. It also scans files that have been compressed using PKLite and LZExe.

For example:

```
FINDVIRU C: /REPAIR
```

scans the C: drive for viruses. If any file viruses are found, the files are repaired if possible. If boot sectors or partition sectors are infected, they are replaced with clean copies.

If any infected files cannot be repaired, FindVirus renames them, changing the first letter of each file extension to a V. For example, FORMAT.COM is change to FORMAT.VOM.

You should check and delete any files with the new extension as soon as possible and restore the original files from clean backups.

Use the `/DELETE` switch to specify that files are to be deleted if they cannot be repaired. For example:

```
FINDVIRU /LOCAL /REPAIR /DELETE
```

scans all local drives for viruses. If any file viruses are found, FindVirus attempts to repair the files. If an original file cannot be repaired, the infected file is deleted. You will then have to restore the original files from a clean backup.

When using FindVirus to repair an infected boot sector or partition sector on a hard disk, you will be prompted to make a recover file:

```
Before we attempt a Boot/Partition sector
repair, it is recommended that you make a
recover file.
Do you wish to make a recover file?
```

If you reply Y, you are prompted to insert a formatted diskette in a A: drive. If you reply N, the repair proceeds without making a recover file.

You can also run FindVirus with the `/BPRESTORE` switch to restore the boot and partition sectors stored in a recover file created earlier. The command has the format:

```
FINDVIR /BPRESTORE
```

You are prompted to confirm the restore and to insert the diskette containing the recover file.

## 11.3 Replacing boot sectors

### How CleanBoot works

CleanBoot replaces the boot sector on a diskette with a valid, non-infected boot sector. You can use this program if FindVirus has reported that a diskette is infected with a boot sector virus.

The single-button repair facility on the user interface also repairs infected boot sectors. See Chapter 6, "If You Find a Virus".

CleanBoot does not delete the boot sector virus, but overwrites the entire boot sector so that the diskette is no longer infectious.

If the virus has made other changes to the diskette, apart from overwriting the boot sector, these will not be undone by running CleanBoot. For example, if the virus has created fake bad sectors to store part of itself, those bad sectors will still be

there. However, this is safe, as code in those sectors can no longer be executed.

If this is the case, use the DOS COPY or XCOPY command to copy the files to a newly-formatted diskette and reformat the original diskette.

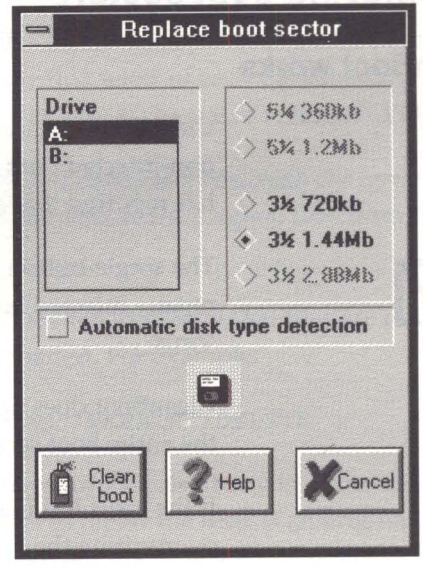
CleanBoot works on 5¼" diskettes of 360 Kb and 1.2Mb capacity, and on 3½" diskettes of 720 Kb, 1.44 Mb and 2.88 Mb capacity.

You can run CleanBoot from the user interface or from the command line.

## Running CleanBoot from the user interface

To replace an infected diskette boot sector from the user interface, follow these steps:

1. Place the diskette you want to repair in the drive.
2. Select Replace boot sector from the Repair drop-down menu. The following screen is displayed:



3. CleanBoot automatically detects the number and type of diskette drives on the PC. Select the appropriate drive in the Drive box.

4. Select the size and capacity of the diskette to be repaired. If you are not sure of the diskette capacity, select Automatic disk type detection. CleanBoot then checks the diskette type itself.

5. The DOS version of the Toolkit allows you to select multiple diskettes. If you choose this, you are prompted to insert another diskette as each one is repaired. To clean multiple diskettes under Windows, press the Clean boot button each time.

6. Select Clean Boot or OK to replace the boot sector.

## Running CleanBoot from the command line

To replace an infected diskette boot sector from the command line, run CLEANBOO from the Toolkit directory. The command has the following syntax:

```
CLEANBOO [drive] [/type] [/NOASM]
```

where:

*drive* is the drive containing the diskette to be repaired.

*type* is one of those in thefollowing table:

| Type | Disk size | Capacity |
|---|---|---|
| 1 | 5¼ | 360 Kb |
| 2 | 5¼ | 1.2 Mb |
| 3 | 3½" | 720 Kb |
| 4 | 3½" | 1.44 Mb |
| 5 | 3½" | 2.88 Mb |
| A | Any | Autodetect |

For example:

```
CLEANBOO B: /4
```

creates a clean boot sector on a 1.44 Mb 3½ diskette in the B: drive.

If you do not specify a drive on the command line, you are prompted for one.

If you do not specify a diskette type, you are prompted to enter one. Press 1 to 5, or A, as indicated in the above table.

If you are not sure of the diskette capacity, press A.

If you select one of the suggested formats and the diskette does not match, CleanBoot detects thist and asks you to confirm that you want to continue. Press Y or N.

When the process has finished, press Y to clean another diskette or N to exit.

## Cross-formatted diskettes

A cross-formatted diskette is one which has been formatted to a different capacity from that for which it was designed.

For example, if a 360 Kb diskette is formatted to 1.2 Mb, running CHKDSK may indicate that there are 800 to 900 Kb of usable space and 300 to 400 Kb in bad sectors. If this diskette is used for storage the data may become inaccessible.

The same problem may occur if a 720 Kb diskette is formatted to 1.44 Mb.

These problems are caused by PCs which cannot distinguish between the two types of diskette because they do not detect the second hole which identifies high-density diskettes.

If you find that files appear to be missing, or that directories are corrupted after running CleanBoot, try running it again with a different diskette capacity. As CleanBoot only affects the boot sector there is no danger of damaging the files on the diskette.

## 11.4 Replacing partition sectors

### How CleanPart works

CleanPart is a diagnostic and repair program which is used to repair partition sectors and hard disk boot sectors which have been infected by a virus.

The single-button repair facility on the user interface will also repair infected partition sectors. See Chapter 6, "If You Find a Virus". Alternatively, you can run FindVirus to repair infected partition sectors as well as files, as explained in "Repairing drives" on page 136.

CleanPart is not virus-specific, but counteracts the effects of most partition sector viruses.

You can use CleanPart in three different ways:

- **Backup**. You can use it to save a copy of the partition sector, boot sector and CMOS data of your hard disk.
- **Restore**. You can use it to restore the partition sector, boot sector and CMOS data from a backup copy made previously.
- **Fix**. If a virus has infected your original partition sector, and you haven't previously made a backup of it, you can use CleanPart to check the disk and create a new partition sector, where possible. Some viruses move the old partition sector elsewhere on the disk, and the Fix option will also search for the old partition sector and replace it.

You can only run CleanPart from the DOS command line. It is not available from the user interface. If you have made a rescue diskette, as described in "Creating a rescue diskette" on page 28, you can also run CleanPart from this diskette.

## Running CleanPart from the command line

The CleanPart command has the following syntax:

```
CLEANPAR [filename] [switches]
```

where:

| | |
|---|---|
| *filename* | indicates the backup file. |
| switches | are as described below. The use of the switches depends on the function you are performing. |

To display help text relating to CleanPart, run the command with the /? switch.

## Backing up partition, boot and CMOS data

To back up the data, run CleanPart from the command line with the /BACKUP or /B option, as follows:

1. Insert a clean, formatted diskette.
2. Run the command:

   ```
   CLEANPAR [filename] /BACKUP [AT]
   ```

   where:

   | | |
   |---|---|
   | *filename* | indicates the backup file. If you do not specify a filename for the backup, CleanPart prompts for one. |
   | AT | must be specified if you want to back up the CMOS data. (This applies to 80286 systems and above; XTs do not have CMOS). |

3. Make sure the backup diskette is clearly labelled, write-protected and kept in a safe place.

For example:

```
CLEANPAR /BACKUP
```

backs up the hard disk's boot and partition data, but not the CMOS. You will be prompted for a filename.

```
CLEANPAR /B=B:DRV.CPB /AT
```

This command backs up up the hard disk's partition and boot sector, and the CMOS data, to the specified file on the B: drive.

The `/BACKUP` function is used to create a rescue diskette. See "Creating a rescue diskette" on page 28.

This backup diskette must only be used to restore data on the PC on which it was created. If you use it on a different PC, you may be unable to access your hard disk.

## Restoring partition and boot sector data

To restore the partition and boot data from diskette, run CleanPart with the `/RESTORE` or `/R` switch.

1. Insert the backup diskette which was produced previously on this PC.
2. Run the command:

   `CLEANPAR` *`filename`* `/RESTORE [AT]`

   where:

   | | |
   |---|---|
   | *`filename`* | indicates the backup file. |
   | `AT` | must be specified if the original backup was created using the `/AT` switch. |

3. You are prompted to confirm that you wish to proceed with the restore. This prompt cannot be suppressed.

4. If the restore is successful, CleanPart prevents you from using the PC until it has been rebooted, so that DOS is updated with the new partition information.

For example:

```
CLEANPAR /R=B:\DRV.CPB /AT
```

will restore the partition, boot and CMOS data previously saved to the file DRV.CPB on the B: drive.

CleanPart uses checksums to verify that the PC to which you are restoring data is the same one from which the backup was made. If the checksums do not match, the data is not restored.

Although this check usually prevents you from restoring partition and boot sectors from a different disk, it is not completely foolproof. If you do succeed in restoring data to a different PC, you may be unable to access your hard disk.

## Restoring CMOS data

To restore just the PC's CMOS data, run CleanPart with the `/RESTORE` switch followed by the `/C` switch.

1. Insert the backup diskette which was produced previously on this PC.
2. Run the command:

   `CLEANPAR [`*`filename`*`] /RESTORE /C [/AT]`

   where

   | | |
   |---|---|
   | *`filename`* | indicates the backup file. If you do not provide a filename for the backup, you are prompted for one. |
   | `/AT` | must be entered if your PC is an 80286 or higher. |

For example:

```
CLEANPAR /RESTORE=B:\DRVC.CPB /C /AT
```

restores the CMOS data from the specified file on the B: drive.

Some PCs, such as PS/2s and other MCA and EISA machine have extended CMOS and the use of the `/AT` switch will give unpredictable results.

There is no way of checking that you are restoring CMOS data to the PC from which the backup was made. If the wrong data is restored, the consequences may be severe. Use this option with great care.

## Replacing the hard disk boot sector

To repair the boot sector of a hard disk, run CleanPart from the command line with the `/H` switch:

```
CLEANPAR /H
```

If the PC hangs while you are attempting a boot sector repair, this may be because the Toolkit's Anti-Stealth Methodology is not compatible with your PC. Power off, boot the PC from a clean, write-protected DOS system diskette and run CleanPart again with ASM turned off:

```
CLEANPAR /H /NOASM
```

## Replacing partition sectors

If a virus has corrupted or moved the partition sector and you don't have a backup to restore from, you can run CleanPart with the `/FIX` option. This works as follows:

- If CleanPart finds a valid partition table on physical sector zero, it creates a new partition sector.
- If there is no valid partition table on physical sector zero, CleanPart searches for a valid one elsewhere on the disk. If it finds one, it copies it to physical sector zero and adds its own version of the partition code.

If no valid partition table is found anywhere on the disk, CleanPart does not attempt to create one.

Before writing a new partition sector, CleanPart forces a backup of the following data:

- The existing partition sector.
- One boot sector, if the disk has a bootable partition.
- The CMOS data (for AT class PCs and above).

To repair the partition sector follow these steps:

1. Insert a clean formatted diskette, to be used as a backup.
2. Run the command:

   `CLEANPAR [`*`disk`*`] [/FIX[=`*`filename`*`]]`

   where:

   *`disk`* specifies the BIOS address of the hard disk. This is only required if you have more than one hard disk and are attempting to repair a hard disk other than the first physical device.

*filename* provides a path for the backup file. If you do not provide a pathname, you are prompted for it.

/FIX prevents the request for confirmation.

3. CleanPart backs up the existing partition sector, boot sector and CMOS data to the diskette. If the backup fails, CleanPart will terminate.

4. It then checks the partition sector and repairs it if possible, as described above.

5. CleanPart then forces a reboot to ensure that the new partition information is available to DOS.

For example:

```
CLEANPAR 129
```

tells CleanPart to check the hard disk at BIOS address 129. The first hard disk is normally at address 128. CleanPart will request confirmation before proceeding, and will prompt for the name of the backup file.

```
CLEANPAR /FIX=A:\DRVC_TBL.CPB
```

tells CleanPart to check the partition sector without prompting for confirmation. The partition, boot and CMOS data will be written to file `DRVC_TBL.CPB` on the diskette in the A: drive.

If the PC hangs while you are attempting a partition sector repair, this may be because the Toolkit's Anti-Stealth Methodology is not compatible with your PC. Power off, boot the PC from a clean, write-protected system DOS diskette and run CleanPart again with ASM turned off:

```
CLEANPAR /NOASM
```

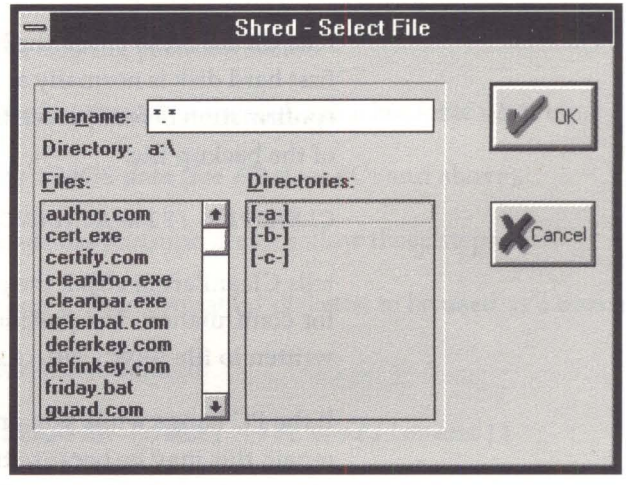
## 11.5 Shredding files

If FindVirus has been unable to repair an infected file, and has changed the first letter of the file extension, you should restore a clean copies from backup and delete the renamed file. To ensure security, it is safer to use the Shred program to delete those infected files.

Shred overwrites a file with a series of characters, and then deletes it. In this way the file cannot be recovered with an Undelete program.

Shred can only be run from the user interface.

Select Shred from the File menu. The following file selection box is displayed:




Select the file to be shredded, and select OK. You asked to confirm the action, since you are not able to restore the file. The file is overwritten and then deleted.

# 12. Using the Toolkit on a Network

This chapter is aimed at network administrators or supervisors. It explains the special requirements and techniques for running the Toolkit on a network.

Network workstations can be infected by file viruses in the same way as standalone PCs. Once a file server is infected, a virus can spread very quickly throughout the network and the damage can be severe.

It is vital to have an effective company anti-virus policy and to ensure that everyone knows what to do if a virus is discovered. For more information, see "What you can do" on page 10.

In general, running the Toolkit on a network is as straightforward as on stand-alone PCs. You should ensure that the Toolkit is installed on all networked PCs (subject to the appropriate site licenses, of course), so that users can scan local hard drives and diskettes. Scan the file servers once a day using FindVirus. ViVerify can be used to check for new viruses.

Network drives can be checked in exactly the same way as local hard disks, except that FindVirus does not need to scan boot sectors. A network does not have boot sectors as the drives are logical rather than physical.

Novell networks can only be infected by a boot sector virus on the server itself.

If you are using Novell NetWare, a specific version of the Toolkit is available to protect servers and workstations. Contact S&S or your authorized distributor.

Additional tips and techniques are described in the rest of this chapter.

## 12.1 Running VirusGuard on a network

It is recommended that VirusGuard is run on all network workstations to prevent viruses from being introduced.

### Use of memory

Use the following guidelines to decide how to run VirusGuard:

- If the workstation has XMS or EMS memory, it does not matter where VirusGuard is run from. The virus driver file in read once, then accessed from additional memory.
- On workstations with no additional memory, VirusGuard should be kept on a local hard disk or RAM drive.
- If your workstation has no hard disk or enhanced memory, it is possible to run VirusGuard from a network drive. However, this results in extra network traffic, which may slow down network response. The workstation will also be noticeably slower during virus scanning.

### Start-up order

On a network workstation you can include the GUARD command in the AUTOEXEC.BAT file, as on a stand-alone PC. Alternatively, include it in a batch file which calls the login command.

Do not include the GUARD command within the login script. Running any TSR within the login script causes the memory area to be split into two parts, resulting in messages such as:

```
Not enough memory to load program
```

You are recommended to run VirusGuard after the network drivers are installed and not before. This is because if the network drivers are installed afterwards, they take over some of the functions that VirusGuard normally intercepts to allow it to examine files. On Novell networks, for example, this usually means that VirusGuard cannot access files on network drives.

If it is not convenient to run VirusGuard after the network drivers, you can run it earlier and then reactivate it after the network drivers are run. You can reactivate VirusGuard using any one of the following methods:

- Run GUARD.COM again with the switch `/REGUARD`.
- Run the command TKUTIL REGUARD.
- Run the command TKUTIL RETSR. See "Restarting TSRs" on page 178.

These three commands all have exactly the same action.

You can automate the reactivation by placing the command at the end of the login script. They are not memory resident themselves. Alternatively, you can place the command in the AUTOEXEC.BAT file, ensuring that it is executed after the point where the network drivers are run.

## Maintaining VirusGuard centrally

It is usually easier to maintain VirusGuard from a central point, to minimize the work involved in upgrading and to ensure that all users have the same version of the software.

To do this, a master version can be kept on a network drive and the workstation users can copy the files to their hard disk or RAM drive each time they log on to the network. When the software is upgraded, the new version can be installed on the network drive and users will automatically copy the new versions.

The easiest way of ensuring this is done is to use the TKUTIL UPDATE command in the workstation's AUTOEXEC.BAT file or the network login script.

This command has the format:

`TKUTIL UPDATE` *`source destination`*

For example:

```
TKUTIL UPDATE U:\TOOLKIT C:\TOOLKIT
```

This command updates all files in C:\TOOLKIT with newer files of the same name in U:\TOOLKIT. For more information on this command, see "Updating files" on page 171.

## Network alarm messages

If you are using a Novell NetWare network, you can configure VirusGuard to send a message to another person whenever the alarm pops up. The default is to send the following message to the network supervisor.

"*username* has had a VirusGuard alarm"

To turn on the messaging feature, you must use the /NET=YES switch.

You can change the default message using the switch:

/NLRT="*message*"

The message must be in quotation marks and can contain up to 40 characters except double quotation marks (") and forward slash (/).

You can send the message to a different person using the switch:

/TELL=*name*

The specified name must be the network identification of the user to whom you want to send the message.

If you use either the /NLRT= or the TELL= options, you do not need to use the /NET=YES option.

If the message cannot be sent for any reason, for example if the user is not logged on, VirusGuard continues as if the network messaging facility had not been switched on.

### Write checks on network drives

Files on network drives are scanned by VirusGuard when they are executed, and optionally when they are copied or read. However the optional `/WRITE` switch does not work when a file is being written to a network drive. This is because DOS treats network drives as devices and the `/WRITE` switch does not scan files being written to devices. You should only rely on the write scan when files are being written to local drives on networked PCs.

### Testing

You can test the operation of VirusGuard on the network drives using a test file. See "Testing VirusGuard" on page 108 for more information. This test can also be used to check the alarm messaging features.

## 12.2 Running FindVirus on a network

If you use FindVirus on a network, options are available to allow a message to be sent to the supervisor or member of the support staff. The default is to send the following message to the network supervisor:

```
username: Virus found on workstation!!!
```

where:

| | |
|---|---|
| *username* | identifies the user of the workstation where the virus was found. |

You can change the default message using the switch:

```
/MSG="message"
```

The message must be in quotation marks and can contain any character except double quotation marks (") and forward slash (/), up to a maximum of 40 characters.

You can change the person to whom the message is sent using the switch:

```
/TELL=name
```

The name must be the network identifier of the recipient, which might be a network administrator or member of the support staff. The username can be in upper or lower case.

For example:

```
FINDVIRU /MSG="Virus alert!!" /TELL=SMITHS
```

## 12.3 Anti-Stealth Methodology

The Toolkit's Anti-Stealth Methodology only works with local drives. To ensure that a stealth virus is not active while you are checking networked drives, you should switch off the PC and reboot from a clean diskette.

## 12.4 Dealing with infected networks

As with any other virus infection, the most important rules are:

- Don't panic
- Don't rush

To clean up the network:

1. Log everyone off the network before the clean-up operation.
2. Scan every workstation for viruses, ensuring you boot from clean, write-protected system diskettes.
3. If the server is running under DOS, run FindVirus on the server itself. If the server is running under OS/2, you can scan the server from a workstation (or use the OS/2 version of the Toolkit).

4. Ensure the entire network is free of viruses before allowing users to log on again.

As for any virus outbreak, the main problem is infected media. You must check all diskettes and make sure all users understand the importance of having their diskettes, including backups, checked.

If you need to reformat the server, do not rely on a single tape backup as these sometimes fail.

# 13. Toolkit Configuration

This chapter explains the configuration files which are used within the Toolkit.

## 13.1 The TOOLKIT.INI file

The TOOLKIT.INI file is used to hold a number of settings for the Toolkit programs. It is loaded automatically when you start the Toolkit. You can edit this file to customize it to your own installation, and you can create other files for different configurations, for example, for different users.

The file is divided into subsections, each of which starts with a heading in square brackets. Beneath each subsection is a list of options defining the current settings.

An example of the TOOLKIT.INI file is as follows:

```
[FindVirus]
Options=BEEP
Report=TOOLKIT.LST
List=FILES.VVL

[FileRepair]
Options=DELETE

[ViVerify]
Options=FILELIST SIZES
Report=VERIFY.REP
List=FILES.VVL
FPrint=FINGERP.VVF
Exclude=EXCLUDE.VVX
```

Note the following points about the format of the file:

- Do not include spaces.
- Where filenames are included, files are assumed to be in the standard Toolkit directory (default C:\TOOLKIT). Alternatively, you can give a full pathname.

The options that can be included are described below.

## FindVirus

| | |
|---|---|
| `Options=switches` | These can be any of the command line switches available for the FINDVIRU command. Do not include the slash character. Options containing an equals sign must be placed on separate lines. |
| `Report=`*`file`* | The output report file. |
| `List=`*`file`* | The file containing the list of files to be scanned. |
| `Driver=`*`file`* | The driver to be used. |

For more information on the available switches, see Chapter 7, "Advanced Virus Detection".

## FileRepair

When FindVirus is run with the file repair option, it always tries to repair an infected file. If the file cannot be repaired, the file can either be renamed or deleted.

| | |
|---|---|
| `Options=` | If you wish to rename files that cannot be repaired, specify RENAME. If you wish to delete files that cannot be repaired, specify DELETE. |

### ViVerify

| | |
|---|---|
| `Options=switches` | Include any of the VIVERIFY command line switches. Do not include the slash character. Options containing an equals sign must be placed on separate lines. |
| `Report=`*`file`* | The output report file. |
| `List=`*`file`* | The file containing the list of files to checked. |
| `Fprint=`*`file`* | The file containing the list of fingerprints. |
| `Exclude=`*`file`* | The file containing the list of files to be excluded from the check. |

For more information on the available switches, see Chapter 9, "Advanced Virus Checking".

## 13.2 The FINDVIRU.INI file

The FINDVIRU.INI file contains options used when you run FINDVIRU with the `/UNPACK` switch to check compressed files.

An example of the FINDVIRU.INI file is as follows:

```
[Options]
ZIP=PKUNZIP.EXE %s *.EXE *.COM /d C:\TZ
ARJ=ARJ.EXE E %s C:\TZ
LZH=LHA.EXE x %s C:\TZ\ *.EXE *.COM
```

The file consists of one line for each compressed file format, for example ZIP and ARJ. When FindVirus encounters files with these extensions, it attempts to decompress them to the temporary directory using the given command line.

For example:

```
ZIP=PKUNZIP.EXE %s *.EXE *.COM /d C:\TZ
```

executes PKUNZIP, which is assumed to be in the same directory as FindVirus. The given filename is substituted for %s and the parameters are passed to PKUNZIP.

Note that although the `/UNPACK` switch can still be used, it has been superseded by the `/PACK` and `/UNZIP` options. See "Compressed and archived files" on page 79 for more information.

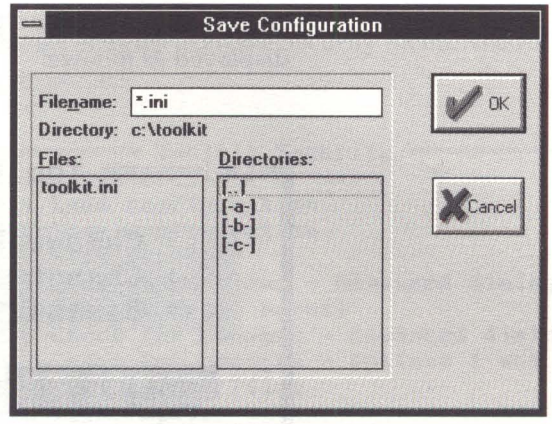
The `/UNPACK` switch is only available on PCs with 386 or higher processors.

## 13.3 Configuration File Management

You can edit TOOLKIT.INI and FINDVIRU.INI using any text editor or word processor that can save the file as unformatted ASCII text.

Alternatively, you can load and save the configuration details held in TOOLKIT.INI from the user interface.

When you have set up a specific set of defaults for FindVirus and ViVerify you can save the settings in a configuration file. Select Save Configuration from the File menu. A file selector box of the following format is displayed:




Provide a name for the file to be saved, and select OK.

By default, the Toolkit loads TOOLKIT.INI when it starts up. To reload a different configuration file, containing previously saved settings, select Load Configuration from the File menu. Select or enter the name of the file to be saved and select OK. The file is loaded and the new settings are applied.

## 13.4 Toolkit security features

A security feature in the Toolkit allows you to disable certain Toolkit features to prevent their use.

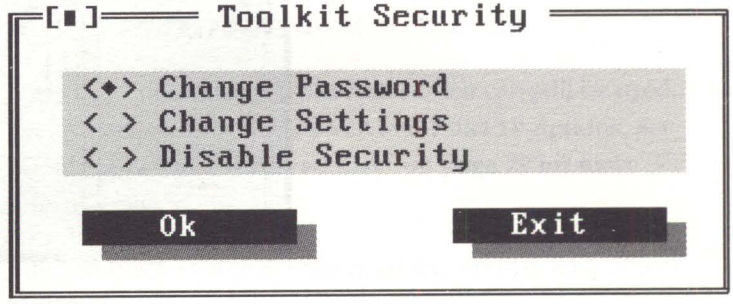
It works by generating a hidden, read-only version of the TOOLKIT.INI file which has a section called `[Misc]` listing the Toolkit functions to be disabled.

The settings apply to both the DOS and Windows versions, but the security features can only be accessed using DOS.

To use the security features, start the Toolkit from the DOS command line as follows:

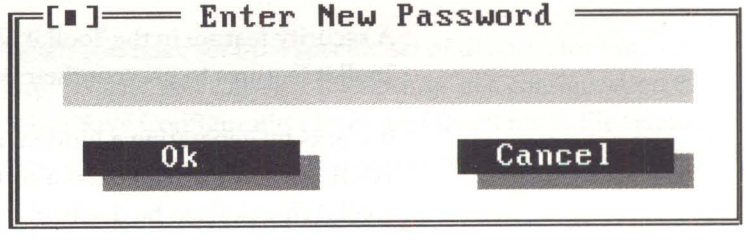
```
TOOLKIT /#S
```

If security features are already enabled, you are prompted to enter the password and press OK. The security menu is displayed as follows:




## To set or change a password

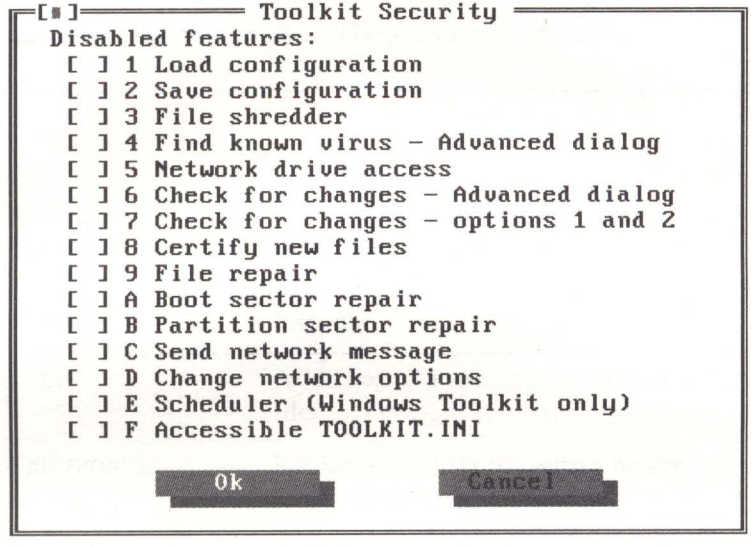
The first time you use the security menu, you have to enter a password. On subsequent occasions, you can change the password if you wish. Select Change password from the Security menu. The following screen is displayed:




Enter a password of at least eight alphanumeric characters. Select OK, then enter it again to confirm.

## To change settings

Select Change settings from the Security menu. The following screen is displayed:


[■] Toolkit Security
Disabled features:
[ ] 1 Load configuration
[ ] 2 Save configuration
[ ] 3 File shredder
[ ] 4 Find known virus - Advanced dialog
[ ] 5 Network drive access
[ ] 6 Check for changes - Advanced dialog
[ ] 7 Check for changes - options 1 and 2
[ ] 8 Certify new files
[ ] 9 File repair
[ ] A Boot sector repair
[ ] B Partition sector repair
[ ] C Send network message
[ ] D Change network options
[ ] E Scheduler (Windows Toolkit only)
[ ] F Accessible TOOLKIT.INI
Ok
Cancel

Features currently disabled are marked by ticks in the left-hand column. Select the items to be disabled by pressing the highlighted key or moving the cursor using the ↓ and ↑ function keys. Then press the space bar.

Select OK to accept the new settings.

If you have disabled features which were available before, you will be asked to enter the password before returning to the Security menu.

If option F, Accessible TOOLKIT.INI has been disabled, the Toolkit automatically sets the file to hidden/system/read-only.

## To disable the security features

If a password has been set, security is automatically enabled. You can disable it by selecting Disable Security from the Security menu.

# 14. Toolkit Utilities

Provided in the Toolkit are a number of utilities which you can run from DOS or within batch files. This chapter explains their purpose and gives examples of how you can use them.

## 14.1 TKUTIL

The TKUTIL utilities are outlined in the table below and explained in more detail in the following sections:

| Utility | Purpose |
|---|---|
| ADD | Adds text to a specified place in a text file. |
| ADUPDATE | Replaces an older file with a newer one of the same name. |
| ALARM | Generates a visible alarm. |
| CPU | Reports the main processor type. |
| DELETE | Deletes a line from a text file. |
| DRIVETYPE | Reports the current disk drive type. |
| FORMFEED | Sends a form feed character to the printer. |
| FROM | Removes references to other anti-virus products from your system files. |
| GUARDCHECK | Indicates whether or not VirusGuard is installed. |
| LASTRUN | Indicates when the program was last run. |
| LOCK | Forces a cold boot of the PC. |
| MEMTYPE | Reports the type of memory installed. |
| MKDIR | Makes a new directory. |

| Utility | Purpose |
|---|---|
| MONTHDAY | Reports the day of the month. |
| REGUARD | Reinitializes VirusGuard after network start-up. |
| RETKEY | Reports the upper-case ASCII keystroke. |
| RETSR | Reinitializes all Toolkit TSRs after network start-up. |
| RFCHECK | Indicates if RingFence is installed. |
| SEARCH | Searches an ASCII file for a given phrase. |
| TECHFILE | Generates a file containing system information. |
| TSRMAP | Returns a list of programs in memory. |
| TUNE | Plays a tune. |
| UPDATE | Replaces an older file with a newer one of the same name. |
| WEEKDAY | Returns the day of the week. |

## Reporting the disk drive

The DRIVETYPE command returns the type of the current disk drive. It has the following syntax:

```
TKUTIL DRIVETYPE
```

The errorlevel returned indicates the type of disk drive, as follows:

| Errorlevel | Disk drive |
|---|---|
| 1 | Diskette drive. |
| 2 | Local fixed disk drive. |
| 3 | Network drive. |

## Reporting the CPU

The CPU command returns the processor type. It has the following syntax:

```
TKUTIL CPU
```

The errorlevel returned indicates the type of CPU installed in the PC, as follows:

| Errorlevel | CPU type |
|---|---|
| 0 | 8086 |
| 2 | 80286 |
| 3 | 80386 |
| 4 | 80486 |
| 5 | Pentium |

## Reporting memory type

The MEMTYPE command returns the type of memory installed. It has the following syntax:

```
TKUTIL MEMTYPE
```

The errorlevel returned indicates the type of memory installed in the PC, as follows:

| Errorlevel | Memory type |
|---|---|
| 0 | Conventional |
| 1 | EMS |
| 2 | XMS |
| 3 | EMS and XMS |

## Reporting Toolkit TSRs

The TSRMAP command lists all the TSRs in memory. It has the following syntax:

```
TKUTIL TSRMAP
```

If you are using DOS 5.0 or above, you can use the `MEM /C` command which has the same function.

## Reporting the latest keystroke

The RETKEY command returns the upper case ASCII code of the current keystroke. You can use this to check if the user has returned a Y or an N in response to a prompt. The command has the following syntax:

```
TKUTIL RETKEY
```

The keystroke is returned as the errorlevel.

## Reporting batch file run

The LASTRUN command indicates when the batch file was last run. You can use it to ensure a program is only run once a day or once a week. For example, if the command is included in `AUTOEXEC.BAT`, it can be used to prevent anti-virus software that was run on start-up from being run again if the PC is rebooted the same day.

It has the following syntax:

```
TKUTIL LASTRUN file
```

where:

| | |
|---|---|
| *file* | is used to store the date information. If no filename is given, the file is called TKUTIL.DAT. |

The command returns the number of days that have elapsed since the program was last run. It returns errorlevel 254 in the following cases:

- If the number of days since the program was last run is greater than 254.
- If the batch program has never been run.
- If it cannot find the specified data file.

## Make new directory

You can use the MKDIR command to create a new directory. The command has the following syntax:

```
TKUTIL MKDIR directory
```

The errorlevels returned are as follows:.

| Errorlevel | Meaning |
|---|---|
| 0 | Directory made successfully. |
| 1 | Directory already exists. |
| 2 | Directory could not be created. |

## Updating files

You can use the UPDATE command or the ADUPDATE command to replace existing files with newer versions. These commands have the following syntax:

```
TKUTIL UPDATE source destination [/A] [/N]

TKUTIL ADUPDATE destination source [/A] [/N]
```

where *source* and *destination* are directory pathnames. The contents of files in the destination directory are replaced with newer files in the source directory with the same name. There are two optional switches:

| | |
|---|---|
| /A | Updates files and add new files in the source directory to the destination directory. |
| /N | Only copies new files in the source directory to the destination directory. |

The UPDATE and ADUPDATE options return the following errorlevels:

| Errorlevel | Meaning |
|---|---|
| 0 | Nothing done. |
| 1 | Files updated but not copied. |
| 2 | Files copied but not updated. |
| 3 | Files copied and updated. |
| 5 | Invalid source directory. |
| 6 | Invalid destination directory. |
| 11 | Insufficient memory. |
| 12 | Source and destination directory identical. |
| 14 | Error during copy. |
| 17 | Empty source directory (ADUPDATE only). |
| 18 | Empty destination directory (UPDATE only). |
| 255 | DOS version/checksum failure. |

## Adding text to a file

You can use the ADD command to add text to a file. This can be used to add entries to AUTOEXEC.BAT or CONFIG.SYS files. It has the following syntax:

```
TKUTIL ADD file 'text' [/START][/END]
[/AFTER 'phrase']
```

where:

*file* is the file to which the text is to be added.

*text* is the text to be added.

One of the optional switches, `/START`, `/END` or `/AFTER` must be given to specify the location of the text.

The ADD command returns the following errorlevels:

| Errorlevel | Meaning |
|---|---|
| 1 | Incorrect parameters. |
| 2 | File not found. |
| 3 | Error reading file. |
| 4 | Error writing file. |
| 5 | The /AFTER switch was included but no text was found. |

Examples of the use of the ADD command are as follows:

```
TKUTIL ADD C:\AUTOEXEC.BAT 'GUARD /COPY=FLOPPY'
/START
```

adds GUARD COPY=FLOPPY to the start of the AUTOEXEC.BAT file.

```
TKUTIL ADD C:\AUTOEXEC.BAT 'GUARD /REGUARD'
/AFTER 'login'
```

adds GUARD /REGUARD to the AUTOEXEC.BAT file after the line containing the text 'login'.

## Deleting text from a file

You can use the DELETE command to delete a specified line of text from a file. It has the following syntax:

```
TKUTIL DELETE file 'text'
```

where:

| | |
|---|---|
| *file* | is the file from which text is to be deleted. |
| *text* | is the line to be deleted. |

The command returns the following errorlevels:

| Errorlevel | Meaning |
|---|---|
| 255 | File error or command line error. |
| 1 | Phrase not found. |
| 0 | Phrase found successfully. |

## Searching for text

The SEARCH command can be used to search for a specified line of text in a file. It has the following syntax:

`TKUTIL SEARCH` *`file`* `'`*`text`*`' where:`

| | |
|---|---|
| *`file`* | is the file to be searched. |
| *`text`* | is the search text. |

The errorlevels returned are as follows:

| Errorlevel | Meaning |
|---|---|
| 255 | File error or command line error. |
| 1 | Text found. |
| 0 | Text not found. |

## Checking VirusGuard

You can use the GUARDCHECK command to check if VirusGuard is installed. It has the following syntax:

```
TKUTIL GUARDCHECK
```

The errorlevels returned are as follows:

| Errorlevel | Meaning |
|---|---|
| 0 | VirusGuard installed. |
| 1 | VirusGuard not installed. |

## Checking RingFence

You can use the RFCHECK command to check if RingFence is installed. RingFence prevents the use of diskettes until they have been checked for viruses on the sheep-dip PC. This authorization can keep out any software, clean or infected. For more information on RingFence, contact S&S.

The RFCHECK command has the following syntax:

```
TKUTIL RFCHECK
```

The errorlevels returned are as follows:

| Errorlevel | Meaning |
|---|---|
| 0 | RingFence installed. |
| 1 | RingFence not installed. |

## Determining the day of the week

The WEEKDAY command can be used to check the day of the week. It has the syntax:

```
TKUTIL WEEKDAY
```

It returns a errorlevel between 1 and 7, as follows:

| Errorlevel | Meaning |
|---|---|
| 1 | Monday |
| 2 | Tuesday |
| 3 | Wednesday |
| 4 | Thursday |
| 5 | Friday |
| 6 | Saturday |
| 7 | Sunday |

## Determining the day of the month

The MONTHDAY command can be used to check the day of the month. It has the syntax:

```
TKUTIL MONTHDAY
```

It returns a errorlevel between 1 and 31 indicating the day of the month.

## Locking the PC

You can use the LOCK command to force a cold boot of the PC if there is a problem. It disables Ctrl + Alt + Del, forcing the user to power off. The LOCK command has the following syntax:

```
TKUTIL LOCK
```

## Sounding an alarm

You can use the ALARM command to generate an alarm if there is a problem. It has the following syntax:

```
TKUTIL ALARM
```

This command causes screens to flash. The time of the alarm is displayed in the centre of the screen.

## Playing a tune

You can use the TUNE command to play one of four different tunes. The command has the following syntax:

```
TKUTIL TUNE n
```

where *n* is a number between 1 and 4.

## Removing other anti-virus packages

If you have previously used other anti-virus software, you can remove any references to them from your system files using the FROM command. The command has the following syntax:

```
TKUTIL FROM [CPAV][NAV][MSAV]
```

where:

| | |
|---|---|
| `CPAV` | removes all references to the Central Point anti-virus package. |
| `NAV` | removes all references to the Norton anti-virus package. |
| `MSAV` | removes all references to the Microsoft anti-virus package. |

The errorlevels returned are as follows:

| Errorlevel | Meaning |
|---|---|
| 255 | File error. |
| 0 | References removed successfully. |

## Send form feed to printer

The FORMFEED command sends a form feed command to the system printer. It has the syntax:

```
TKUTIL FORMFEED
```

The errorlevels returned are as follows:

| Errorlevel | Meaning |
|---|---|
| 1 | No printer attached. |
| 0 | Form feed sent successfully. |

## Restarting VirusGuard

You may need to use the REGUARD command if you run VirusGuard on a network. If you start up VirusGuard before logging in to the network it may not work properly, and you should ensure it is reactivated. The REGUARD command reactivates VirusGuard. It has the following syntax:

```
TKUTIL REGUARD
```

You should place this command at the end of the login script. For more information, see "Running VirusGuard on a network" on page 152.

## Restarting TSRs

You may need to use the RETSR command if you run VirusGuard on a network. It reactivates the TSRs after logging on to the network, ensuring they work correctly. The command has the following syntax:

```
TKUTIL RETSR
```

You should place this command at the end of the login script. Note that if you use RETSR, you do not need to use REGUARD as well. For more information, see "Running VirusGuard on a network" on page 152.

## Reporting technical information

The TECHFILE command generates a file of system information, including the contents of your AUTOEXEC.BAT and CONFIG.SYS files. You may be asked for this by S&S Technical Support staff if you have a problem.

The command has the following syntax:

```
TKUTIL TECHFILE file
```

where *file* specifies the file to be created. If you do not give a filename, the file will be called TECHDATA.S&S.

## 14.2 Examples of batch files

Four sample batch files are included on the installation disks. You can run them as they are, modify them for your own use or use them as examples of how to write your own batch files.

They are as follows:

- VIV1.BAT which runs the ViVerify FILELIST and MAKEPRINT functions.
- VIV2.BAT which runs the ViVerify CHECKPRINT function.
- FRIDAY.BAT which shows you how to run Toolkit functions on specific days of the week.
- FV.BAT which runs FindVirus.

The listings are included here for reference.

### VIV1.BAT

```
@Echo off
rem Run ViVerify to create filelist
VIVERIFY FILELIST /D=C
rem Now run ViVerify to make the signatures
VIVERIFY MAKEPRINT /D=C /N=5
rem
rem See the manual for documentation on the
rem other ViVerify switches
rem
Echo Now you can run the VIV2 batch file
Echo to check the disk
```

## VIV2.BAT

```
@Echo off
VIVERIFY CHECKPRINT /D=C /N=5
rem
rem See the manual for documentation on the
rem other ViVerify switches
rem
IF ERRORLEVEL = 255 GOTO INT
IF ERRORLEVEL = 3 GOTO PROBLEM
IF ERRORLEVEL = 2 GOTO VIRUS
IF ERRORLEVEL = 1 GOTO PROBLEM
IF ERRORLEVEL = 0 GOTO CLEAR
:INT
Echo ViVerify interrupted by user
GOTO EXIT1
:VIRUS
ECHO Change detected. Please call your
ECHO PC Support person
GOTO EXIT1
:PROBLEM
ECHO There has been some problem (not a virus)
ECHO with ViVerify
ECHO Please call your PC Support person
GOTO EXIT1
:CLEAR
ECHO Virus check completed - all clear
:EXIT1
```

## FRIDAY.BAT

```
Rem This batch file shows you how to make one
Rem thing happen on Fridays, and something
Rem else on other days of the week. You can
Rem use it for controlling the running of
Rem Toolkit programs
TKUTIL WEEKDAY
IF ERRORLEVEL = 7 GOTO FRIDAY
IF ERRORLEVEL = 6 GOTO NOTFRIDAY
IF ERRORLEVEL = 5 GOTO NOTFRIDAY
IF ERRORLEVEL = 4 GOTO NOTFRIDAY
IF ERRORLEVEL = 3 GOTO NOTFRIDAY
IF ERRORLEVEL = 2 GOTO NOTFRIDAY
IF ERRORLEVEL = 1 GOTO NOTFRIDAY
IF ERRORLEVEL = 0 GOTO NOTFRIDAY
: NOT FRIDAY
Rem Today is not Friday. Run the non-Friday
Rem programs now
Rem Remember that if you call another batch
Rem file, use "CALL BATCHFILE"
GOTO EXIT1
:FRIDAY
Rem Today is Friday. Run the Friday programs
Rem now; for example:
FINDVIRU C:
Rem And here you can test the Errorlevel,
Rem as in the FV.BAT file
:EXIT 1
```

## FV.BAT

```
@Echo off
FINDVIRU /D=C
rem
IF ERRORLEVEL = 255 GOTO INT
IF ERRORLEVEL = 3 GOTO PROBLEM
IF ERRORLEVEL = 2 GOTO VIRUS
IF ERRORLEVEL = 1 GOTO PROBLEM
IF ERRORLEVEL = 0 GOTO CLEAR
:INT
Echo FindVirus interrupted by user
GOTO EXIT1
:VIRUS
ECHO Change detected. Please call your
ECHO PC Support person
GOTO EXIT1
:PROBLEM
ECHO There has been some problem
ECHO (not a virus) with ViVerify
ECHO Please call your PC Support person
GOTO EXIT1
:CLEAR
ECHO Virus check completed - all clear
:EXIT1
```

# 15. Reference Information

This chapter includes reference information, including the command line syntax and switches for all the Toolkit commands.

## 15.1 TOOLKIT command

### Syntax

```
TOOLKIT [switches]
```

### Switches

| Switch | Meaning |
|---|---|
| /G | Display in greyscale. |
| /ID | Load Inspect Disk. |
| /M | Display in monochrome. |
| /NOASM | Turn off Anti-Stealth Methodology. |
| /NV | Use block mouse pointer instead of arrow. |
| /VE | Load Virus Encyclopedia. |
| /#S | Security options (for more information, see "Toolkit security features" on page 163). |

## 15.2 FINDVIRU command

### Syntax

```
FINDVIRU [switches]
```

### Switches

| Switch | Meaning |
|---|---|
| /ALLDRIVES | Check all fixed disk drives, including network drives. |
| /ANALYZE | Use heuristic scanner. |
| /BADLIST=*file* | Write suspect filenames to the specified file. |
| /BEEP | Beep when a virus is found. |
| /CHECKLIST=*file* | Check files listed in specified file. |
| /D=drives | Check specified drives. |
| /DOALLFILES | Check all files, not just executables. |
| /DRIVER=*file* | Use named virus driver file. |
| /EXTERROR | Provide extended error levels. |
| /EXTRA=*file* | Use specified additional virus driver. |
| /FORCEFLOPPY | Force reading of diskette boot sector when diskette is changed. |
| /GURU | Provide a list of files compressed using PKLite, LZExe and other packages. |
| /HELP<br>/? | Display the most common FindVirus switches. |
| /INI | Read parameters from INI file |
| /LOCAL | Check local hard disk drives. |
| /LOUD | Display status of each file scanned. |

| Switch | Meaning |
|---|---|
| /MSG=*message* | Send message to the network supervisor. |
| /NOBOOT | Do not scan boot or partition sector. |
| /NOFILES | Disable file scanning. |
| /NOMSG | Disable network broadcast. |
| /NOPACK | Do not scan files compressed with PKLite and LZExe. |
| /NOPART | Do not check partition sectors. |
| /ONEONLY | Check one diskette only. |
| /ONVIRUS=HALT<br>/ONVIRUS="*msg*" | Carry out the specified action if a virus is found. |
| /PACK | Scan files compressed with PKLite, LZExe, ICE, Diet or CryptCom. |
| /PAUSE | Pause for keystroke before scanning. |
| /PRINTOUT | Output report to the printer as well as to the screen. |
| /REPAIR[/DELETE] | Repair infected files. The optional /DELETE switch deletes files that cannot be repaired. |
| /REPORT=*file* | Output report to specified file. |
| /SILENT | Suppress screen output. |
| /SUMMARY | Produce a summary report. |
| /TELL=*name* | Send network messages to user. |
| /UNPACK | Scan compressed files. (Superseded by /UNZIP and /PACK.) |
| /UNZIP | Scan files compressed or archived ARC, ICE, Diet, LZH or CryptCom. |
| /YESBREAK | Enable interruption with Ctrl Break. |

## 15.3 GUARD command

### Syntax

```
GUARD [switches]
```

### Switches

| Switch | Meaning |
|---|---|
| /COPY=NO<br>/COPY=YES<br>/COPY=FLOPPY<br>/COPY=LOCAL<br>/COPY=ALL | Define whether or not files are to be scanned when they are copied and read. |
| /CODE="*code*" | Check diskettes for authorization code. |
| /FON | Scan Windows font files. |
| /MODE=EMS | Force use of EMS memory. |
| /MODE=DISK | Force use of hard disk. |
| /NET=YES | Send default network messages. |
| /NLRT="*message*" | Specify a network alert message. |
| /NWA=YES | Enable NLM communications. |
| /REGUARD | Reactivate VirusGuard. |
| /STRICT | Prevent access to unauthorized diskettes. Must be used with the /CODE switch. |
| /TELL="*user*" | Specify a network user name for alert messages. |
| /WARN="*message*" | Display a warning message. |
| /WRITE=NO<br>/WRITE=YES<br>/WRITE=FLOPPY<br>/WRITE=LOCAL<br>/WRITE=ALL | Define whether or not files are to be scanned when they are written. |

## 15.4 VIVERIFY command

### Syntax

```
VIVERIFY function [switches]
```

where:

| | |
|---|---|
| `function` | is one of FILELIST, MAKEPRINT, CHECKPRINT or AUTOMAKE. |

### Functions

| | |
|---|---|
| `FILELIST` | Make a list of the files to check. |
| `MAKEPRINT` | Calculate the fingerprints for the listed files. |
| `CHECKPRINT` | Check the files in the list for changes. |
| `AUTOMAKE` | Perform `FILELIST` and `MAKEPRINT` functions in one operation. This function is not available in the Windows version. |

### Switches

| Switch | Meaning |
|---|---|
| `/ASM` | Use Anti-Stealth Methodology. |
| `/BADLIST` | Create a list of files that have changed. |
| `/BEEP` | Beep when a changed file is encountered. |
| `/CRC` | Use the CCITT Cyclic Redundancy Check algorithm (default). |
| `/D=` | Specify the drive(s) to be checked. |
| `/DES` | Use the DES algorithm. |
| `/EXCLUDE=`*`file`* | Exclude all files listed in specified file from fingerprinting or checking. |

| Switch | Meaning |
|---|---|
| /EXTERROR | Provide extended error levels. |
| /FL=*file* | Create a file list (FILELIST function) or check files in list (AUTOMAKE, MAKEPRINT, CHECKPRINT functions). |
| /FS=*file*<br>/FPRINT=*file* | Define file holding the fingerprints. |
| /HOLDKEY | Wait for a keystroke before displaying the report. |
| /LOUD | Display status of each file checked. |
| /N=n | Check every nth byte of each file. |
| /NETVOL | Exclude unreadable network files from a file list. |
| /NOBOOT | Do not check boot sector. |
| /NOPART | Do not check partition sector. |
| /NT | Do not use turbo mode; check entire contents of file. |
| /PRINTOUT | Output report to printer as well as to screen. |
| /REPORT=*file* | Output report to specified file as well as screen. |
| /SIZES | Use the file size algorithm. |
| /WHOLESUM | Use the whole sum algorithm. |
| /X=*keyword* | Specify the keyword to be used. |
| /YESBREAK | Enable interruption of ViVerify with Ctrl Break. |

## 15.5 CLEANPAR command

### Syntax

```
CLEANPAR [file] [switches]
```

where:

*file* indicates the backup file.

### Switches

| Switch | Meaning |
|---|---|
| /AT | Backup or restore CMOS data. Used with /BACKUP and /RESTORE. |
| /BACKUP<br>/B | Backup partition sector, boot sector data and, optionally, CMOS data. |
| /C | Restore CMOS data; used in conjunction with /RESTORE. |
| /FIX<br>/F | Repair the partition sector, if possible, suppressing confirmation prompts. |
| /H | Replace hard disk boot sector. |
| /NOASM | Disable Anti-Stealth Methodology. |
| /RESTORE<br>/R | Restore partition sector and boot sector. |
| /? | Display the most common CLEANPAR switches. |

## 15.6 CLEANBOO command

### Syntax

```
CLEANBOO [drive] [/type] [/NOASM]
```

where:

| | |
|---|---|
| *drive* | is the drive containing the diskette to be repaired. |
| type | is a number between 1 and 5 or the letter A, to indicate the diskette type. See "Running CleanBoot from the command line" on page 141. |

### Switches

| Switch | Meaning |
|---|---|
| /NOASM | Disable Anti-Stealth Methodology |

## 15.7 WTKUTIL command

### Syntax

```
WTKUTIL [switches] COMMAND [switches] [optional
parameters ...] switches
```

### Switches

| Switch | Meaning |
|---|---|
| `/help or /?` | display help, then continue with valid commands, if any |

### Commands

#### ADD

```
WTKUTIL ADD WINGUARD path
```

Modify WIN.INI and the registry to enable WinGuard next time the PC is rebooted. WinGuard must be in the specified path.

#### REMOVE

```
WTKUTIL REMOVE WINGUARD
```

Modify WIN.INI and the registry to disable WinGuard next time the PC is rebooted.

#### WINGUARDCHECK

```
WTKUTIL WINGUARDCHECK
```

Display a message indicating whether or not WinGuard is loaded. Return error level 1 if WinGuard is loaded, error level 2 otherwise.

### SAVESETTINGS

```
WTKUTIL SAVESETTINGS WINGUARD filename
```

Write WinGuard's settings to the specified file, in text format. Return error level 255 if the file or registry section cannot be opened, error level 0 for a successful operation.

### LOADSETTINGS

```
WTKUTIL LOADSETTINGS WINGUARD filename
```

Delete the current WinGuard settings and replace them with those read from the specified file. Return error level 255 if the file cannot be opened, error level 0 for a successful operation. (This command does not enable WinGuard.)

### CHECKSETTINGS

```
WTKUTIL CHECKSETTINGS WINGUARD filename
```

Compare WinGuard's current settings with those stored in the specified file. Return error level 1 if the settings are the same, error level 2 if they are different, error level 255 if the file or registry section cannot be opened.

# Glossary

| | |
|---|---|
| alias | A different name by which a *virus* is known. |
| AT | A PC based on the 80286 processor. |
| ASM | Anti-Stealth Methodology™. Facilities included in the Toolkit to detect viruses that use *stealth*. |
| AUTOEXEC.BAT | A *batch program* that specifies a set of commands that are executed every time you start up the PC. |
| backup | A copy of your data held in another place in case your working copy is lost or damaged. |
| batch program | A file containing a set of DOS commands that you can run by typing just one command. Batch files have the file extension BAT. |
| BBS | Bulletin Board System. An electronic mail system used to send messages and transfer files. |
| BIOS | Basic Input/Output System. Permanent programs that are used to load DOS when the system is started up. |
| boot | Start the computer. |
| boot diskette | A diskette containing operating system files which can be used to start up your computer. |

| | |
|---|---|
| boot sector | The part of every hard disk and diskette that is read by the computer when it starts up. |
| boot sector virus | A virus transmitted in the *boot sector* of a diskette. Boot sector viruses infect the boot sectors of hard disks, and often the *partition sectors* as well. |
| bug | An unintentional fault in a program. |
| caching | A way of speeding up the amount of time a program spends accessing the hard disk. Part of the memory is used as a temporary store. |
| CARO | Computer Anti-Virus Researchers Organisation. Several members of S&S are members of CARO. |
| checksummer | A program that looks for viruses by checking for changes in *executable files*. ViVerify is an example of a checksummer. |
| clean | Free from viruses. |
| cluster | The minimum allocation unit on a disk, usually consisting of 2, 4 or 8 *sectors*. |
| CMOS | An area of storage used to hold system setup details in PCs with a 286 processor or above. CMOS is non-volatile memory, which means that its contents are not lost when the PC is powered off. |

| | |
|---|---|
| cold reboot | Rebooting the system by turning off the PC and turning it on again. This is normally recommended when running the Toolkit as some viruses can survive a *warm reboot.* |
| COM file | An *executable file* with a file extension of COM. |
| COMMAND.COM | The DOS command line processor which carries out the commands that you type in. |
| CONFIG.SYS | A file in the root directory which specifies which devices to install and which *device drivers* to use. |
| conventional memory | Up to 640 Kb of memory which is used by DOS for its basic commands. Also known as base memory. |
| cylinder | All the *tracks* on a disk which are the same distance from the centre. |
| defragmenters | A program which reorganizes a hard disk so that different *clusters* of each file are stored contiguously if possible. This improves disk efficiency. |
| device driver | A DOS program used to control the items of hardware connected to the PC such as disk drives and printers. Some device drivers are built into DOS, and others can be added. |
| directory | A logical subdivision of a disk which organizes files into groups. DOS holds information on files within a directory which can be displayed by the DIR command. |

| | |
|---|---|
| disk compressor | A program which stores files in a compressed form to maximize space on the hard disk. |
| dropper | A file which is not itself a virus, but infects the PC. |
| driver file | A file used by the Toolkit to enable the identification and reporting of viruses. |
| EICAR | European Institute for Computer Anti-Virus Research. S&S is a member of EICAR. |
| enhanced memory | Memory installed on the PC in addition to the *conventional memory*, either extended memory or expanded memory. |
| EXE file | An *executable file* with the file extension EXE. |
| executable file | A file containing a program which can be run by typing its filename at the DOS command line. |
| expanded memory | A type of memory which can be installed in addition to *conventional memory*. Available on 286-based PCs and above. Commonly known as EMS. |
| extended memory | A type of memory which can be installed in addition to *conventional memory*. Commonly known as XMS. |
| false alarm | A report of a virus where none exists. |
| fast infectors | A file virus that infects programs when they are opened or copied as well as when they are run. |

| | |
|---|---|
| FAT | File Allocation Table. The area on a disk which holds information on which *clusters* on the disk belong to which file. |
| file virus | A virus which infects *executable files*. When the program is run the virus copies itself. Most file viruses are *memory resident*. |
| fingerprint | A unique numeric identifier for a file; used by *checksummers* to check for changes in executable files. Also known as a checksum. |
| footbath PC | A PC used to check incoming files and diskettes for viruses. Also known as a sheep-dip PC. |
| format | The method of preparing a disk before files are written to it, using the DOS FORMAT command. The command creates a *root directory* and a *FAT*. |
| GDE | Generic Decryption Engine. An element of FindVirus which enables it to identify even the most complex polymorphic encrypted viruses. |
| head | One of the read/write coils in a disk drive. |
| heuristic scanner | An element of FindVirus that checks files for suspicious code which may indicate a new virus. |
| hexadecimal | Representation in base 16. |
| infected file | A file containing a virus. |
| interrupt | The way in which programs ask DOS and the *BIOS* to perform a task. |

| | |
|---|---|
| joke programs | Practical joke programs. These are not viruses, but sometimes a virus is contained in a joke program. The Toolkit detects joke programs. |
| logic bombs | A type of *trojan* that is triggered by a particular set of circumstances. |
| low-level format | A *BIOS* level format. Unlike a DOS format, this erases all the contents and partition information of a hard disk. |
| macro file | A data file containing instructions that specify actions to be taken by an applications program. |
| macro virus | Any virus, similar to the Concept virus, that infects data files, for example, Word 6 document files. |
| Master Boot Record | The partition sector of a hard disk. |
| memory resident | A program which remains in the PCs memory once it has run. Also known as *TSR*. |
| multi-partite virus | A virus which uses a combination of techniques to spread, for example, infecting both files and *boot sectors*. |
| mutant | A slight variation of a known virus. |
| overwriting virus | A virus which overwrites each file it infects. |
| partition sector | The first part of a hard disk to be read. This contains the location of each partition, and the number of sectors in each one. |
| partition sector virus | A virus that replaces the normal *partition sector* of a hard disk. |

| | |
|---|---|
| polymorphic virus | A virus that tries to evade detection by scanners by ensuring that it does not have a fixed pattern of bytes. The Toolkit can detect polymorphic viruses using the Generic Decryption Engine. |
| public domain software | Software which you can copy and distribute legally. |
| RAM drive | An area in memory which emulates a hard disk drive, but with faster access. |
| rescue diskette | A diskette used to restore the *partition sector, boot sector* and *CMOS* of your hard disk if they have been infected by a virus. |
| root directory | The topmost directory on a disk, where all other directories and files are stored. |
| scanner | A virus detection program that searches for known viruses. FindVirus is an example of a scanner. |
| sector | A part of a *track*, usually 512 bytes long. |
| shareware | Software which you can copy legally, but must pay for if you decide to use it. |
| sheep-dip PC | A PC used to check incoming files and diskettes for viruses. Sometimes called a footbath PC. |

| | |
|---|---|
| stealth | Characteristic of a virus which tries to avoid detection. Stealth viruses interfere with DOS and *BIOS interrupts* in order to conceal their presence. |
| SYS file | File, generally a *device driver*, with an extension of SYS. |
| time bombs | A type of *trojan* that is triggered by a particular date. |
| track | All the *sectors* around the disk on a single *head* and at a the same distance from the centre. |
| trojan | A program that has an unexpected action. Trojans are not viruses, as they do not replicate, but they are often damaging and are detected by the Toolkit. |
| TSR | Terminate and Stay Resident. A program that remains in memory after it has run. |
| upgrade | A new version of the Toolkit which has been updated to detect newly-discovered viruses. Upgrades are available quarterly or monthly. |
| variant | A variation of a virus, usually caused by amending the code of an existing virus. |
| virus | A program that replicates itself. |
| warm reboot | Restarting the PC by pressing Ctrl Alt and Del at the same time. Some viruses, for example, Joshi, can survive a warm reboot. |

| | |
|---|---|
| write-protect | Ensuring that files cannot be written to a disk. A 5¼" diskette is write-protected by placing a label over the notch. A 3½" diskette is write-protected by sliding a plastic tab to uncover a hole. |
| XT | PC based on the 8086 processor. |

# Index


A
ADD command 172
adding text to a file 172
Advanced menu 39
alarm 176
ALARM command 176
algorithm 63, 122
aliases 6
Anti-Stealth Methodology
  device driver 133
  explanation 132
  on a network 156
  turning off 133
  turning on 133
  with CleanPart 147
  with Inspect Disk 129
  with ViVerify 124
anti-virus policy 10, 151
ARC 84, 137
archived files 55, 79, 84, 161
ARJ 55, 84, 137, 161
ASCII keystroke 170, 171
Author
  command syntax 114
  how it works 112
  purpose 14
  running 113
  using with VirusGuard 102
authorization code 102, 112
AUTOEXEC.BAT 21, 27, 96, 152

B
backup diskettes 91, 113
backups 9, 10, 18
base memory. See conventional memory
batch files
  examples 179
  FRIDAY.BAT 181
  FV.BAT 182
  reporting previous run 170
  VIV1.BAT 179
  VIV2.BAT 180
boot diskette xviii
Boot Repair menu option 38
boot sector 3
  explanation 3
  FindVirus checks 85
  repair 75, 139
  replacing 140
  virus 3
  VirusGuard checks 99
  ViVerify checks 120
booting from diskette 33, 51, 75
bugs 7
bulletin boards 7, 11

C
CARO 6
changed files 61
Check for Changes menu option 38
Check Memory menu option 38
checking day of the month 176
checking memory 125
checking RingFence 175
checking VirusGuard 174
checking week of the month 175
Checksum algorithm 63, 116
checksummers 12, 115
checksums 14, 57, 146
CLEANBOO command
  switches 190, 191
  syntax 141, 190
CleanBoot
  how it works 139
  purpose 15
  running from the command line 141
  running from the user interface 140
CLEANPAR command
  switches 189
  syntax 189
  use 144–149
CleanPart
  backing up data 143
  fixing damaged partition sector 143
  how it works 143
  purpose 15
  repairing hard disk boot sector 147
  restoring data 143
  running from the command line 144
clean-up operation 156
closing the Toolkit 36
CMOS 11, 28, 144, 148
companion virus 4
compressed files 55, 79, 84, 161

Computer Anti-Virus Researchers Organisation 6
CONFIG.SYS 21, 29, 107, 133
configuration file management 162
configuration files 56, 64, 159
conventional memory 24, 96, 107
conventions xvii
CPU command 169
CPU type 169
CRC algorithm 63, 116, 122
cross-formatted diskettes 142
CryptCom 84, 137
Cyclic Redundancy Check. See CRC

D
Data Encryption Standard. See DES
DELETE command 173
deleting files 137, 150
deleting text from a file 173
DES algorithm 64, 116, 122
dialog boxes xxi
Diet 84, 137
disabling Toolkit features 163
disk drive type 168
disk sector editor 110
disk space xviii, 19
diskettes 6, 11, 139, 142
DOS system diskette xviii, 33, 51, 75, 77, 132, 135, 147, 149
DOS Toolkit xix, 18, 31
downloading software 11
Dr Solomon's xxx
driver file 104
DRIVETYPE command 168
dropper 5

E
EMS. See expanded memory
encrypted files 80
encryption algorithm 116
errorlevels
  FindVirus 89, 90
  ViVerify 124
examining disks 126
executable files 79, 98, 115
Exit menu option 37
expanded memory 24, 47, 96, 104, 152
extended memory 24, 47, 96, 104, 152
EXTRA.DRV 88

F
false alarms 92
fast infectors 3
File menu 37
file repair
  from the command line 138
  from the user interface 136
file selection xxii
file virus 2
Find Viruses menu option 38
FINDVIRU command
  switches 81–89, 184
  syntax 138, 184
FINDVIRU.DRV 88
FINDVIRU.INI
  editing 162
  example 161
  explanation 161
FindVirus
  advanced menu options 54
  command syntax 81
  configuration file 160
  driver file 88
  error messages 92
  errorlevels 90
  executable files 79
  hints and tips 90
  how it works 77
  network options 87
  purpose 13, 41, 51
  repairing files 80
  reporting 53, 73, 85
  reporting viruses 73
  running from the command line 81
  running from the main screen 52
  running from the user interface 53, 81
  scanning specific drives 82
  scanning specific files 83
  scheduling scans 67
  speeding up 91
  switches 81–89
  testing 92, 108
  when to use 51
fingerprint 14, 57, 63, 115, 116
FON files 102
FORMFEED command 177
FRIDAY.BAT 181
FROM command 177
FV.BAT 182

G
games 7, 12
Generic Decryption Engine 6
GUARD command
  adding to AUTOEXEC.BAT 27, 96
  switches 100–106, 186
  syntax 100, 186
GUARD.COM 24, 95
GUARD.DRV 24, 95, 104
GUARDCHECK command 174
GuardMem
  purpose 14, 125
  running from the command line 125
  running from the menu 125
GUARDMEM.COM 125

H
help text xxvi
human error 9

I
ICE 84, 137
Inspect Disk
  advanced options 128
  menu option 39
  purpose 14, 126
  running from the command line 129
  running from the user interface 126
Inspect File
  menu option 39
  purpose 14, 129
  running 129
Inspect Memory
  menu option 39
  purpose 15, 131
  running 131
installation
  DOS 18
  options 17
  upgrades 31
  VirusGuard 24
  VirusGuard and WinGuard 20
  Windows 18
installing the Toolkit 17

J
joke programs 9

K
keyword 57, 121

L
LASTRUN command 170
LCD screen 34
listing TSRs 170
Load Configuration menu option 37
loading configuration file 163
LOCK command 176
locking the PC 176
logic bomb 9
login script 152
low-level programs 8
LZExe 55, 84, 137
LZH 84, 137

M
main screen 36, 52
Master Boot Record 3
MEM command 25, 47
MEM.DRV 125
memory checking 125
memory type 169
memory-resident virus 125
MEMTYPE 169
MESSAGES.DRV 24, 95
MONTHDAY command 176
mouse xix
multipartite virus 5

N
network
  alarm messages 154
  Anti-Stealth Methodology 156
  drive 25, 48, 152
  running FindVirus 155
  running VirusGuard 152
  start-up order 152
  using the Toolkit 151
  virus infection 7, 156
Novell NetWare xxvii, 151, 154

O
on-line help xxvi
OS/2 xxvii, 156
overwriting virus 5

**P**
partition sector
explanation 3
FindVirus checks 85
repair 76, 143
replacing 143
virus 4
ViVerify checks 120
partition sector viruses 3
PC configuration xviii
pirated software 11
PKLite 55, 84, 137
PKZIP 55, 84, 161
PKZip 137
polymorphism 5
pop-up alarm 46, 47, 48, 71
preventing access to diskettes 103

**R**
RAM drive 25, 27, 48, 152
reactivating VirusGuard 153
README files xxx, 8, 30
reference information 183
registration xxix
REGUARD command 153, 178
renaming files 75, 137
Repair Drive menu option 38
Repair menu 38
repairing
boot sectors 75, 139
drives 136
files 75, 80, 88, 136
from user interface 75
partition sectors 76, 143, 148
single button 75
single-button 135, 139, 143
Replace Boot Sector menu option 38
replacing
boot sectors 139
partition sectors 143
reporting batch file runs 170
rescue diskette 28, 143, 145
restarting VirusGuard 178
restoring CMOS data 146
restoring partition and boot sectors 145
RETKEY 170, 171
RETSR command 153, 178
RFCHECK command 175
RingFence 175

**S**
S&S, contacting xxx
save configuration file 162
Save Configuration menu option 37
Scan menu 38
scanners 12
scanning specific files 83
Schedule menu option 39
scheduling
FindVirus 67
under Windows 67
ViVerify 68
SEARCH command 174
searching for text 174
security features
changing settings 165
disabling 165
menu 164
passwords 164
purpose 163
start-up 163
security levels 106
shareware 7
sheep-dip PC 13, 80, 112
short-cut keys xx
Shred
purpose 15
running from the user interface 150
Shred menu option 37
single-button repair 75, 135, 139
Size algorithm 63, 116, 122
software sources 11
sounding the alarm 46, 48, 71, 176
spoofing 57, 116
starting the Toolkit 33
stealth 5
system configuration xviii

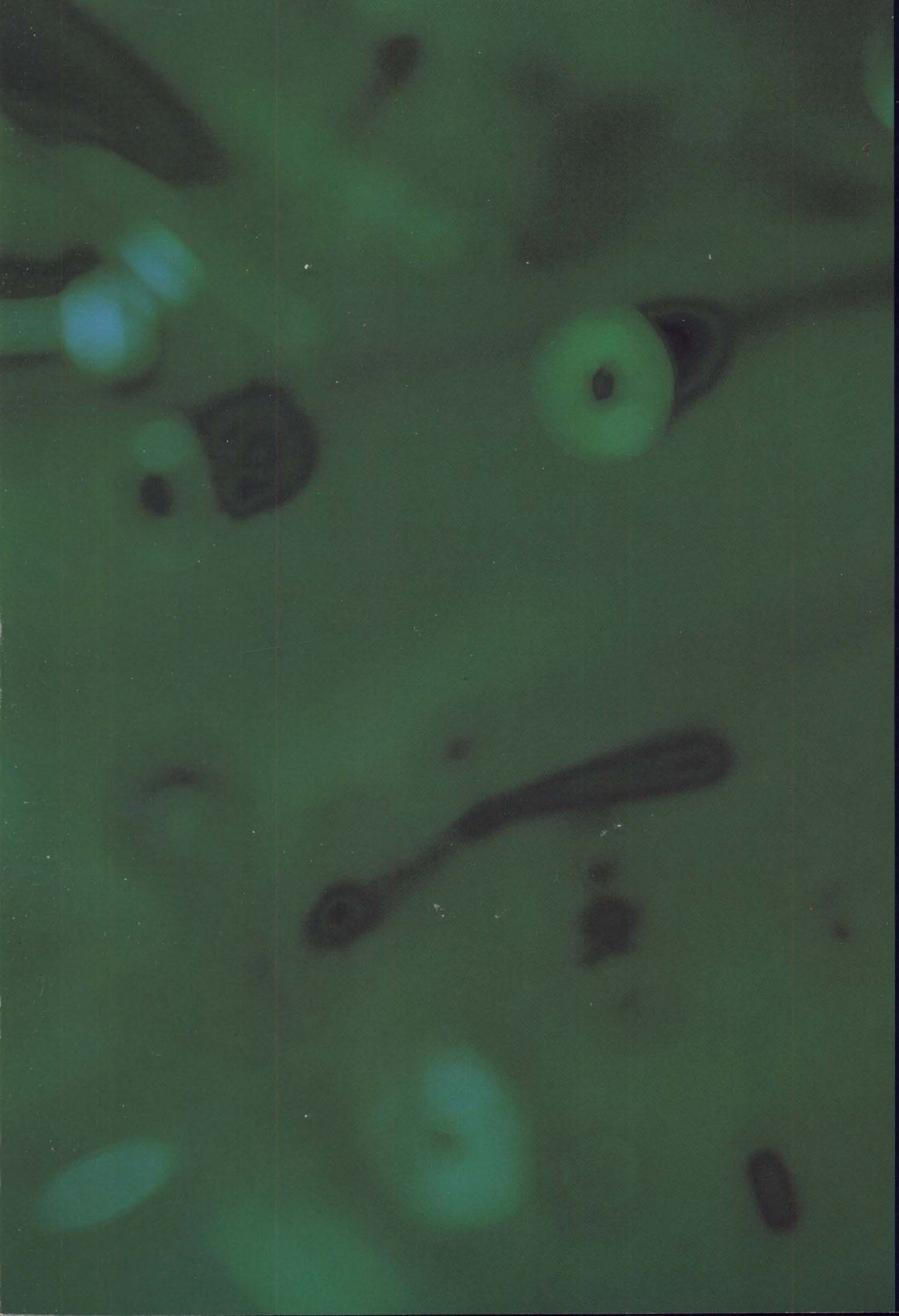
**T**
TECHDATA.S&S 178
TECHFILE command 178
technical data 178
technical support xxx, 23, 76, 92
test file 108
testing FindVirus 108
testing VirusGuard 108
time bomb 9
TKUTIL
ADD 167, 172

ADUPDATE 167
ALARM 167, 176
CPU 167, 169
DELETE 167, 173
DRIVETYPE 167, 168
explanation 167
FORMFEED 167, 177
FROM 167, 177
GUARDCHECK 167, 174, 175
LASTRUN 167, 170
LOCK 167, 176
MEMTYPE 167, 169
MKDIR 167, 171
MONTHDAY 168, 176
REGUARD 153, 168, 178
RETKEY 168, 170, 171
RETSR 153, 168, 178
RFCHECK 168, 175
SEARCH 168, 174
TECHFILE 168, 178
TSRMAP 168, 170
TUNE 168, 176
UPDATE 153, 168, 171
WEEKDAY 168, 175
toolbar xxiii, xxiv, 126
Toolkit
configuration 159
directory 19
DOS version xix, 18, 31
running from diskette 17
utilities 167
Windows version xix, 18, 32
TOOLKIT command
switches 183
syntax 183
TOOLKIT.INI
editing 162
example 159
explanation 159
TOOLKIT.SYS 133
trojans 8
TSR. See memory-resident
TSRMAP command 170
TUNE command 176
turbo mode 64, 116, 121

U
unrepairable files 75, 138
UPDATE command 153, 171
updating files 153, 171
upgrades xxix, 31, 93, 112
user interface 36
using the keyboard xx
utilities 167

V
variants 6, 66
virus
characteristics 5
definition 1
names 6, 66
prevention 10
reporting 71
side effects 2
stealth 132
types 2
Virus Encyclopedia xxiii, xxvii, 5, 14, 65
Virus Encyclopedia menu option 39
VirusGuard
checking diskette authorisation 102
error messages 111
executable files 23, 98
hints and tips 106
how it works 95
installation 20, 24
loading high 107
maintaining centrally 153
memory requirements 24
network use 105, 152
on network drive 25
pop-up alarm 71
purpose 13
reactivating 153
reporting 46, 48, 71
running 26, 96, 100
security levels 22, 98
switches 100–106
system requirements 95
testing 108, 155
use of memory 96
VIV1.BAT 179
VIV2.BAT 180
ViVerify
advanced menu options 62
algorithms 63, 116, 122
AUTOMAKE function 117, 118
checking speed 116, 121
CHECKPRINT function 117

command line switches 118
computing fingerprints 59, 60, 117
configuration file 161
creating file list 59, 117
error levels 123
errorlevels 124
excluding files 63, 120
executable files 115
FILELIST function 117
how it works 115
keyword 59, 121
MAKEPRINT function 117
purpose 14, 57
reporting 74, 122
running from the command line 117
running from the user interface 58, 117
scheduling checks 68
suspect files 123
verifying fingerprints 59, 61, 117
when to use 57
VIVERIFY command
functions 187
switches 118, 187
syntax 117, 187

W
WEEKDAY command 175
Windows
icons xxiii, 35
schedule 67
toolbar xxiv, 126
Windows Toolkit xix, 18, 32
WinGuard 42
Windows alarm 72
workstations 151
WTKUTIL command
commands 191
switches 191
syntax 191

X
XMS. See extended memory
XT xviii, 21, 95